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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Secure Auditing and Avoid Deduplication Datain Cloud

Sudhir Manikrao Thombre, Prof. Mr. Sathish kumar Penchala

Department of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Pune, India

ABSTRACT: As the cloud computing innovation creates amid the foremost recent decade, outsourcing info to cloud administration for capability turns into Associate in Nursing tempting pattern, that benefits in saving endeavors on substantial info repairs and administration, In any case, following the outsourced cloud warehousing isn't fully reliable, it raises security worries on the for most skillful technique to acknowledge info deduplication in cloud whereas accomplishing uprightness examining. during this work, we tend to think over the difficulty of honesty examining and secure deduplication on cloud info. Specifically going for accomplishing each info uprightness and deduplication in cloud, we tend to propose protected frameworks, to be specific SecCloud and SecCloud+. SecCloud presents Associate in Nursing examining substance with Associate in Nursing repairs of a Map Reduce cloud, that assists customers with manufacturing info labels before transferring and additionally review the honesty of knowledge having been place away in cloud. Contrasted and past work, the calculation by shopper in SecCloud is hugely lessened amid the file transferring and reviewing stages. SecCloud+ consists propelled by the method that purchasers perpetually got to scramble their info before transferring, and empowers honesty evaluating and secure deduplication on encoded inform.

KEYWORDS: Secure Deduplication, Integrity Auditing, Cloud Computing, Proof of Ownership.

I. INTRODUCTION

Despite the very fact that cloud storage framework has been usually embraced, it neglects to oblige some important rising wants, as an example, the capacities of auditing integrity of cloud files by cloud customers and detection derived files by cloud servers. we tend to show each problems beneath.

The first issue is integrity auditing. The cloud server has the capability alleviate customers from the substantial weight of capability administration and maintenance. The foremost distinction of cloud storage from customary in-house storage is that the information is changed by means that of web and place away in an unsure domain, not in check of the purchasers by any stretch of the imagination, that inevitably raises customer extraordinary worries on the integrity of their information. These worries originate from the manner that the cloud storage is defenceless to security dangers from each outside and within the cloud, and also the uncontrolled cloud servers may inactively conceal some information misfortune incidents from the purchasers to take care of their infamy. Additionally real is that for saving money and house, the cloud servers could even effectively and advisedly lose once during a whereas ought to information files happiness to a normal client. Considering the substantial size of the outsourced information files and also the customers' forced quality skills, the first issue is summed up as in what manner will the client efficiently perform periodical integrity verifications even while not the neighbourhood duplicate of knowledge files.

II. LITRATURE SURVEY

1]Title :1. Iris: A Scalable Cloud File System with Efficient Integrity Checks
Authors: Emil Stefanov, Marten van Dijk.
Iris, a sensible, real organisation designed to support workloads from huge enterprises storing info inside the cloud and be resilient against probably devious service suppliers. As a transparent layer imposing strong integrity guarantees, Iris lets academic degree enterprise tenant maintain associate degree oversize organisation inside the cloud. In Iris, tenants acquire strong assurance not merely on info integrity, but to boot on info freshness, still as info retrievability simply just in case of accidental or adversarial cloud failures. Iris offers academic degree style ascendable to many purchasers (on the order of a full bunch or maybe thousands) issue operations on the organisation in parallel. Iris includes new

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

optimization and enterprise-side caching techniques specifically designed to beat the high network latency typically veteran once accessing cloud storage. Iris to boot includes novel erasure cryptography techniques for economical support of dynamic Proofs of Retrievability (PoR) protocols over the organisation. Authors describe style and experimental results on a epitome version of Iris. Iris achieves end-to-end turnout of up to 260MB per second for 100 purchasers issue coincident requests on the organisation. (This limit is settled by the offered network metric and most drive turnout.) we tend to tend to demonstrate that strong integrity protection inside the cloud are going to be achieved with borderline performance degradation.

2] Title. StealthGuard: Proofs of Retrievability with Hidden Watchdogs
Authors: Monir Azraoui, Kaoutar Elkhiyaoui, Refik Molva
This paper presents StealthGuard, associate economical and incontrovertibly secure proof of irretrievability (POR) theme. StealthGuard makes use of a privacy protective word search (WS) rule to go looking, as a part of a POR question, for randomly-valued blocks known as watchdogs that ar inserted within the file before outsourcing. because of the privacy-preserving options of the WS, neither the cloud supplier nor a 3rd party unwelcome person will guess that watchdog is queried in every POR question. Similarly, the responses to POR queries also are obfuscated. thence to answer properly to each new set of POR queries, the cloud supplier needs to retain the get in its completeness. StealthGuard stands out from the sooner sentinelbased POR theme planned by Juels and Kaliski (JK), owing to the employment of WS and also the support for an infinite range of queries by StealthGuard. The paper additionally presents a proper security analysis of the protocol.

3]Title:An Efficient Proof of Retrievability with Public Auditing in Cloud Computing
Authors: Jin Li, Xiao Tan, Xiaofeng Chen
This paper presents StealthGuard, associate economical and incontrovertibly secure proof of retrievabillity (POR) theme. StealthGuard makes use of a privacy protective word search (WS) rule to go looking, as a part of a POR question, for randomly-valued blocks known as watchdogs that ar inserted within the file before outsourcing. because of the privacy-preserving options of the WS, neither the cloud supplier nor a 3rd party unwelcome person will guess that watchdog is queried in every POR question. Similarly, the responses to POR queries also are obfuscated. thence to answer properly to each new set of POR queries, the cloud supplier needs to retain the get in its completeness. StealthGuard stands out from the sooner sentinelbased POR theme planned by Juels and Kaliski (JK), owing to the employment of WS and also the support for an infinite range of queries by StealthGuard. The paper additionally presents a proper security analysis of the protocol.

4]Title: Reclaiming Space from Duplicate Files in a Serverless Distributed File System
Authors: John R. Douceur, Atul Adya, William J. Bolosky, Dan Simon
The Farsite distributed filing system provides handiness by replicating every file onto multiple desktop computers. Since this replication consumes important space for storing, it's vital to reclaim used house wherever doable. activity of over five hundred desktop file systems shows that almost half all consumed house is occupied by duplicate files. Authors gift a mechanism to reclaim house from this incidental duplication to create it on the market for controlled file replication. This mechanism includes 1) focussed coding, that allows duplicate files to amalgamate into the house of one file, even though the files area unit encrypted with totally different users' keys, and 2) dish, a Self- composition, Lossy, Associative info for aggregating file content and placement data during a decentralised, scalable, fault-tolerant manner. Large-scale simulation experiments show that the duplicate-file coalescing system is ascendible, extremely effective, and fault-tolerant

5]Title: Identity-Based Encryption from the Weil Pairing
Authors: Dan Boneh, Matthew Franklin
Authors propose a completely purposeful identity-based coding theme (IBE). The theme has chosen ciphertext security within the random oracle model forward a variant of the machine Diffe-Hellman downside. this technique relies on linear maps between teams. The Weil pairing on elliptic curves is associate degree example of such a map. Author provide precise definitions for secure identity primarily based coding schemes and provides many applications for such systems.

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

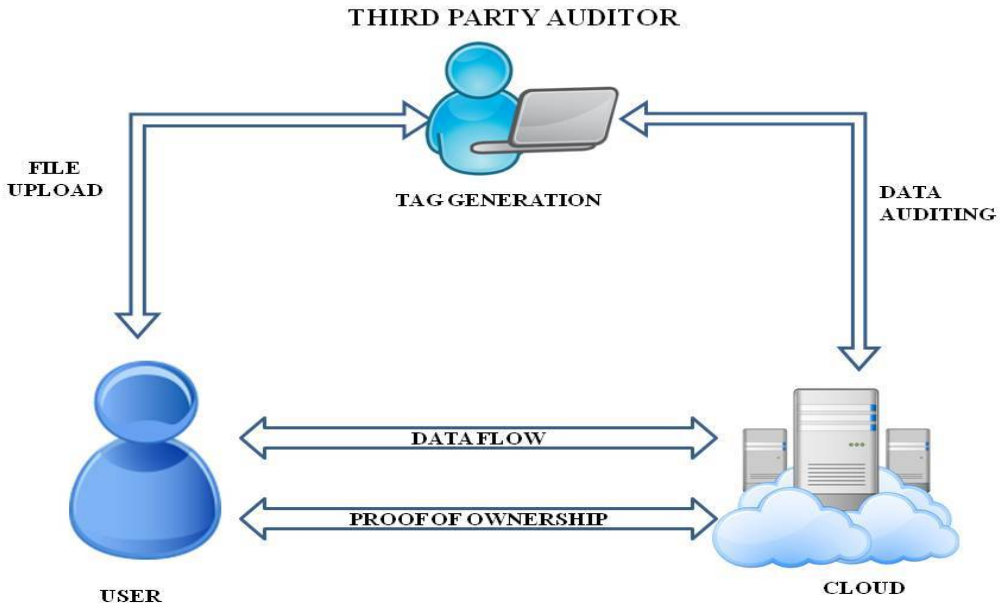
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

III. PROPOSED SYSTEM

We indicate that our proposed SecCloud framework has accomplished both trustworthiness examining and file deduplication. On the other hand, it can't keep the cloud servers from knowing the substance of files having been put away. As such, the functionalities of uprightness inspecting and secure deduplication are just forced on plain files. In this area, we propose SecCloud+, which considers honesty evaluating and deduplication on scrambled files. Framework Model Compared with SecCloud, our proposed SecCloud+ includes an extra trusted element, to be specific key server, which is in charge of doling out customers with mystery key (as indicated by the file content) for scrambling files. This building design is in accordance with the late work. In any case, our work is recognized with the past work by taking into consideration trustworthiness reviewing on scrambled information. SecCloud+ takes after the same three conventions (i.e., the file transferring convention, the respectability reviewing convention and the verification of possession convention) as with SecCloud. The main contrast is the file transferring convention in SecCloud+ includes an extra stage for correspondence between cloud customer and key server. That is, the customer needs to correspond with the key server to get the merged key for scrambling the transferring file before the SecCloud.



Advantages of Proposed System:

1. It provides the Integrity auditing by clustering the files with removing the duplicate files.
2. The duplicate files are mapped with a single copy of the file by mapping with the existing file in the cloud.

IV. OBJECTIVE

1. File Confidentiality. The design goal of file confidentiality requires to prevent the cloud servers from accessing the content of files. Specially, we require that the goal of file confidentiality needs to be resistant to“dictionary attack”. That is, even the adversaries have pre-knowledge of the “dictionary” which includes all the possible files, they still cannot recover the target file

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

2. Integrity Auditing
3. Secure Deduplication
4. Cost-Effective

V. MOTIVATION

We verify that our projected SecCloud framework has accomplished each integrity auditing and file deduplication. Be that because it could, it cannot keep the cloud servers from knowing the substance of files having been place away. In alternative words, the functionalities of integrity auditing and secure deduplication area unit simply forced on plain files. during this space, we tend to propose SecCloud+, that takes into consideration integrity auditing and deduplication on disorganized files. Framework Model Compared with SecCloud, our projected SecCloud+ involves an additional trustworthy component, to be specific key server, that is answerable of assignment customers with mystery key (according to the file content) for encrypting files. This construction modeling is in line with the late work. However, our work is distinguished with the past work by permitting integrity auditing on encoded knowledge. SecCloud+ takes once constant 3 protocols (i.e., the file uploading protocol, the integrity auditing protocol and also the proof of proprietary protocol) like SecCloud. the most distinction is that the file uploading protocol in SecCloud+ involves an additional stage for correspondence between cloud client and key server. That is, the client must speak with the key server to induce the incorporate key for encrypting the uploading file before the innovate SeeCloud.

VI. CONCLUSION

Aiming at achieving each knowledge integrity and deduplication in cloud, we have a tendency to propose SecCloud and SecCloud+. SecCloud introduces AN auditing substance with maintenance of a Map Reduce cloud, that assists customers with generating knowledge labels before uploading and to boot reviews the integrity of information having been place away in cloud. Moreover, SecCoud empowers secure deduplication through introducing a symptom of possession protocol and preventing the discharge of aspect channel info in knowledge deduplication. Contrasted and past work, the calculation by consumer in SecCloud is implausibly diminished throughout the file uploading and auditing stages. SecCloud+ could be a propelled development persuaded by the means that purchasers perpetually have to be compelled to code their knowledge before uploading, and takes under consideration integrity auditing and secure deduplication squarely on disorganized knowledge

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFRENCES

[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
[5] 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.
[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 12:1–12:34, 2011.
[7] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, ser. SecureComm '08. New York, NY, USA: ACM, 2008, pp. 9:1–9:10.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

[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.