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. 4, Issue 12, December 2016

A Survey on Dynamic Proof of Storage in Multiple Users Environment

Nita Jadhav, Prof. Shyam Gupta

M. E Student, Dept. of Computer Engineering, Siddhant College of Engineering, Sudumbare, Pune, Maharashtra, India

Professor, Dept. of Computer Engineering, Siddhant College of Engineering, Pune, Sudumbare, Maharashtra, India

ABSTRACT: Dynamic Proof of Storage (PoS) could be a helpful scientific discipline primitive that allows a user to see the integrity of outsourced files and to with efficiency update the files in a very cloud server. Though researchers have planned several dynamic PoS schemes in single user environments, the matter in multi-user environments has not been investigated sufficiently. A sensible multi-user cloud storage system wants the secure client-side cross-user deduplication technique, that permits a user to skip the uploading method and procure the possession of the files now, once alternative house owners of an equivalent files have uploaded them to the cloud server. To the simplest of our data, none of the present dynamic PoSs will support this system. during this paper, we have a tendency to introduce the conception of deduplicatable dynamic proof of storage associated propose an economical construction referred to as DeyPoS, to realize dynamic PoS and secure cross-user duplication, at the same time. Considering the challenges of structure diversity and personal tag generation, we have a tendency to exploit a unique tool referred to as Homomorphic genuine Tree (HAT). We have a tendency to prove the protection of our construction, and therefore the theoretical analysis and experimental results show that our construction is economical in follow.

KEYWORDS: Deduplication, Proof of ownership, Dynamic proof of storage, Cloud Computing

I. INTRODUCTION

Storage outsourcing is turning into additional and additional enticing to each trade and tutorial because of the benefits of low value, high accessibility, and straightforward sharing. Collectively of the storage outsourcing forms, cloud storage gains wide attention in recent years. Several firms, like Amazon, Google, and Microsoft, give their own cloud storage services, wherever users will transfer their files to the servers, access them from varied devices, and share them with the others. Though cloud storage services are wide adopted in current days, there still stay several security problems and potential threats .Data integrity is one among the foremost vital properties once a user outsources its files to cloud storage. Users ought to be convinced that the files keep within the server don't seem to be tampered. Ancient techniques for safeguarding knowledge integrity, like message authentication codes (MACs) and digital signatures need users to transfer all of the files from the cloud server for verification that incurs a significant communication value. These techniques don't seem to be appropriate for cloud storage services wherever users could check the integrity oftentimes, like each hour. Thus, researchers introduced Proof of Storage (PoS) for checking the integrity while not downloading files from the cloud server. What is more, users may need many dynamic operations, like modification, insertion, and deletion, to update their files, whereas maintaining the potential of PoS. Dynamic PoS is projected for such dynamic operations. In distinction with PoS, dynamic PoS employ structures, like the Merkle tree. Thus, once dynamic operations are dead, users regenerate tags (which are used for integrity checking, like MACs and signatures) for the updated blocks solely, rather than create for all blocks. To rised perceive the subsequent contents. We tend to gift additional details concerning PoS and dynamic PoS. In these schemes, every block of a file is hooked up a (cryptographic) tag that is employed for substantiating the integrity of that block. Once a champion desires to ascertain the integrity of a file, it every which way selects some block indexes of the file, and sends them to the cloud server. Consistent with these challenged indexes, the cloud server returns the corresponding blocks beside their tags. The champion checks the block integrity and index correctness. The previous are often directly bonded by cryptanalytic tags. a way to affect the latter is that the major distinction between PoS and dynamic PoS In most of the PoS schemes, the block index is “encoded” into its tag, which implies the champion will check the block integrity and index

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. 4, Issue 12, December 2016

correctness at the same time. However, dynamic PoS cannot cypher the block indexes into tags, since the dynamic operations could modification several indexes of non-updated blocks that incurs reserve computation and communication value. As an example, there's a file consisting of one thousand blocks, and a replacement block is inserted behind the second block of the file. Then, 998 block indexes of the first file are modified, which implies the user should generate and send 999 tags for this update. Structures are introduced in dynamic PoSs to unravel this challenge. As a result, the tags are hooked up to the structure instead of the block indexes .However, dynamic PoS remains to be improved in an exceedingly multi-user atmosphere, because of the necessity of cross-user American state duplication on the client-side. This means that users will skip the uploading method and acquire the possession of files now, as long because the uploaded files exist already within the cloud server. This method will cut back space for storing for the cloud server, and save transmission information measure for users. To the simplest of our data, there are no dynamic PoS that may support secure cross-user American state duplication.

II. RELATED WORK

1] Title:A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data
Authors: Zhihua Xia, Xingming Sun, Qian Wang
In this paper, a secure, economical and dynamic search mechanism is projected, that supports not solely the correct multi-keyword hierarchical search however conjointly the dynamic deletion and insertion of documents. We have a tendency to construct a special keyword balanced binary tree because the index, and propose a "Greedy Depth-first Search" algorithmic program to get higher potency than linear search. Additionally, the parallel search process is administered to additional scale back the time price. the safety of the theme is protected against 2 threat models by exploitation the secure kNN algorithmic program. Experimental results demonstrate the potency of our projected theme. There is a unit still several challenge issues in radial SE schemes. Within the projected theme, owner is chargeable for generating change information and causation them to the cloud server.

2] Title: Security and Privacy in Cloud Computing: A Survey
Authors: Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou
Cloud Computing becomes a buzzword nowadays. More and more companies step into Cloud and provide services above on it. However, security and privacy issues impose strong barrier for users' adoption of Cloud systems and Cloud services. We observed the security and privacy concerns presented by an amount of Cloud Computing system providers in this paper. Nevertheless, those concerns are not adequate. More security strategies should be deployed in theCloud environment to achieve the 5 goals (i.e. availability, confidentiality, data integrity, control and audit) as well as privacy acts should be changed to adapt a new relationship between users and providers in the Cloud literature.

3]Title:From Security to Assurance in the Cloud: A Survey
Authors: Claudio ardagna , Rasool asal.
Cloud tenants will use cloud resources at lower costs, and better performance and adaptability, than ancient on-premises resources, while not having to worry concerning infrastructure management. Still, cloud tenants stay involved with the cloud's level of service and therefore the non-functional properties their applications will judge. Within the previous couple of years, the analysis community have been specializing in the non-functional aspects of the cloud paradigm, among which cloud security stands out. Many approaches to security are delineate and summarized generally surveys on cloud security techniques. The survey during this article focuses on the interface between cloud security and cloud security assurance. First, we offer a summary of the state of the art on cloud security. Then, we have a tendency to introduce the notion of cloud security assurance and analyse its growing impact on cloud security approaches. Finally, we have a tendency to gift some recommendations for the event of next-generation cloud security and assurance solutions

4]Hybrid Provable Data Possession at Untrusted Stores in Cloud Computing
Authors: Narn - Yih Lee,Yun - Kuan Chang
We centered the core problems, if Associate in Nursing untrusted server to store client data. we will demonstrable information possession within the model, that scale back the info block access, however conjointly scale back the

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. 4, Issue 12, December 2016

number of computation on the server and shopper and server traffic. Our style and development on the PDP program is especially supported the usage of symmetrical and uneven cryptography system. It exceeds what we have a tendency to die within the past the advance has delivered to the information measure, computation and storage system. And it applied the general public (third party) verification. Finally, we have a tendency to conjointly expect our program, it supports dynamic outsourcing of data build it an additional realistic application of cloud computing atmosphere.

III. PROPOSED ALGORITHM

No Such system of Dynamic proof of storage will achieve cross user deduplication. To remove these drawbacks we implement Deduplicatable dynamic proof of storage.

A. SYSTEM MODEL

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.
As shown in Fig. 2. for every file, original user is that the user World Health Organization uploaded the file to the cloud server, whereas ulterior user is that the user World Health Organization established the possession of the file however didn't truly transfer the file to the cloud server. There square measure 5 phases during a deduplicatable dynamic PoS system: pre-process, upload, deduplication, update, and proof of storage.

B. PRE-PROCESS PHASE

Users will transfer their native files. The cloud server decides whether or not these files ought to be uploaded. If the transfer method is granted, enter the transfer phase; otherwise, enter the deduplication part.

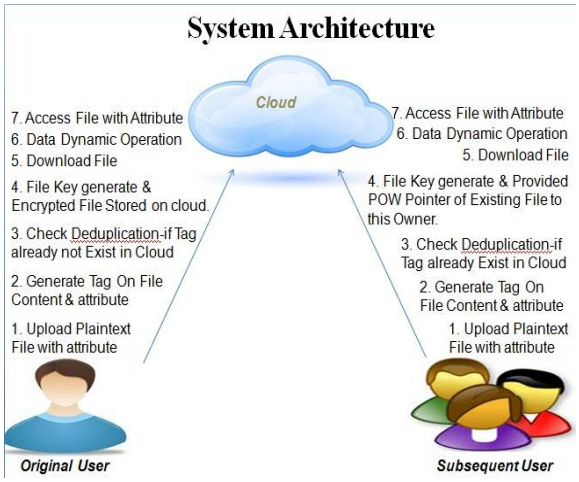

Fig.1. System architecture

C. UPLOAD PHASE

Users will transfer their native files. The cloud server decides whether or not these files ought to be uploaded. If the transfer method is granted, enter the transfer phase; otherwise, enter the deduplication part.

D. DEDUPLICATION PHASE

The files to be uploaded exist already within the cloud server. the next users possess the files domestically and also the cloud server stores the structures of the files. ulterior users got to persuade the cloud server that they own the files while not uploading them to the cloud server. If these 3 phases (pre-process, upload, and deduplication) square measure dead

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. 4, Issue 12, December 2016

just one occasion within the life cycle of a file from the angle of users. That is, these 3 phases seem only if users will transfer files. If these phases terminate unremarkably, i.e., users end transfering within the upload part, or they pass the verification within the deduplication part, we are saying that the users have the ownerships of the files.

E. ***UPDATE PHASE***

Users could modify, insert, or delete some blocks of the files. Then, they update the corresponding components of the encoded files and also the structures within the cloud server, even the first files weren't uploaded by themselves. Note that, users will update the files provided that they need the ownerships of the files, which suggests that the users ought to transfer the files within the transfer part or pass the verification within the deduplication. For each update, the cloud server needs to reserve the first file and also the structure if there exist different homeowners, and record the updated a part of the file and also the structure. this permits users to update a file at the same time in our model, since every update is barely "attached" to the first file and structure.

F. ***PROOF OF STORAGE***

Users solely possess a little constant size information domestically and that they need to examine whether or not the files square measure dependably hold on within the cloud server while not downloading them. The files might not be uploaded by these users however they pass the deduplication part and prove that they need the ownerships of the files. Note that, the update part and also the proof of storage part will be dead multiple times within the life cycle of a file. Once the possession is verified, the users will randomly enter the update part and also the proof of storage part while not keeping the first files domestically.

IV. **CALCULATION**

Let S be the Whole system which consists,
S= {I, P, O}
Where,
I-Input,
P- procedure,
O- Output.
I-{F,Q}
F-Filesset of {f1,f2,…,fn}
Q- Users Query{q1,q2,……,qN}

Procedure(P):
Where :
F = represents the file,
m1,m2,m3,m4=represents the i- th block of the file,
e=encryption key.

Step 1: Pre-process Phase
In the pre-process phase,
e ←H(F), id ←H(e).
Then, the user announces that it has a certain file via id. If the file does not exist, the user goes into the upload phase. Otherwise, the user goes into the deduplication phase.

Step 2 The Upload Phase
Let the file F = (m1, . . . ,mn).
The user first invokes the encoding according
(C, T) ←Encode(e, F)

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. 4, Issue 12, December 2016

Step 3. The Deduplication Phase
If a file announced by a user in the pre-process phase exists in the cloud server, the user goes into the deduplication phase and runs the deduplication protocol
$res \in \{0, 1\} \leftarrow \text{Deduplicate}\{U(e, F), S(T)\}$

Step: 4 The Update Phase
In this phase, a user can arbitrarily update the file, by invoking the update protocol
$res \in \{he*, (C*, T*)i, \perp\} \leftarrow \text{Update}\{U(e, \iota, m, OP), S(C, T)\}$

Step 5: The Proof of Storage Phase
At any time, users can go into the proof of storage phase if they have the ownerships of the files. The users and the cloud server run the checking protocol
$res \in \{0, 1\} \leftarrow \text{Check}\{S(C, T), U(e)\}$

Output(O):
User can upload, download update on cloud server and provide data dedupliaction.

V. CONCLUSION

We planned the great necessities in multi-user cloud storage systems and introduced the model of deduplicatable dynamic PoS. we had develop a unique tool known as HAT that is Associate in Nursing economical genuine structure. Supported HAT, we had planned the primary sensible deduplicatable dynamic PoS theme known as DeyPoS and evidenced its security within the random oracle model. The theoretical and experimental results show that our DeyPoS implementation is economical, particularly once the file size and therefore the range of the challenged blocks area unit giant.

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.

REFERENCES

1. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2016.
2. Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 843859, 2013.
3. C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From Security to Assurance in the Cloud: A Survey," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 2:1–2:50, 2015.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. of CCS*, pp. 598–609, 2007.
5. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in *Proc. Of SecureComm*, pp. 1–10, 2008. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in *Proc. of ASIACRYPT*, pp. 319–333, 2009.
6. C. Erway, A. K¨upc ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. of CCS*, pp. 213–222, 2009.
7. R. Tamassia, "Authenticated Data Structures," in *Proc. of ESA*, pp. 2–5, 2003.
8. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS*, pp. 355–370, 2009.
9. F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, "Outsourced proofs of retrievability," in *Proc. of CCS*, pp. 831–843, 2014.
10. H. Shacham and B. Waters, "Compact Proofs of Retrievability," *Journal of Cryptology*, vol. 26, no. 3, pp. 442–483, 2013.