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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Deduplication with Security Using Target and Global side Techniques

S.Hemalatha[1], K. Manjamadevi [2]

Assistant Professor, Department of Computer Science Engineering, Karpagam College of Engineering, India[1]

Assistant Professor, Department of Master of Computer Applications, Karpagam College of Engineering, India[2]

ABSTRACT: Data deduplication is a method of sinking luggage needs by eliminating redundant data. Only one unique occasion of the data is actually retained on storage transmit in cloud.outmoded data is replaced with a pointer to the unique data copy and it has been far and wide used in cloud packing to reduce the amount of storage space and save bandwidth .Backups are failing, taking too much position , and costing way too much. In the open systems world, these are the same distribute we had years ago, when the first data deduplication technology first entered the unconventional Today, data the amount of space are growing more rapid and organisations of every size are struggling to manage what has become a very luxurious problem. To defeat these issues in this paper we are proposed powerful deduplication practice for the secure storage in cloud using target and global side techniques.

KEYWORDS: Deduplication, secure storage, backup, cloud.

I. INTRODUCTION

Cloud computing provides apparently not limited virtualized resources to users as services across the whole Internet, while whacking platform and implementing an individual fact or item. Today's cloud service provider's bid both decidedly available storage and extraordinarily parallel computing resources at relatively low costs. As cloud computing becomes rampant, an increasing quantity of data is being stored in the cloud and shared by users with itemize privileges, which define the access rights of the stored data. One uncertain challenge of cloud storage services is the management of the ever-increasing volume of data[3]. To make data supervision accessible in cloud computing, deduplication has been well known technique and has fascinated more and more loyal recently. Data deduplication is a generalized data compression technique for eliminating duplicate copies of recurring uniformly over a surface data in storage, the technique is used to steps forward storage.

Mistreatment and can also be applied to network data transfer to degree the number of bytes that must be sent. Instead of keeping respective data copies with the same content, deduplication eradicate redundant data by keeping only one physical copy and mention other redundant data to that copy.

To avert unconstitutional access, a secure proof of ownership the official procedure is also needed to provide the proof that the user indeed owns the counterpart content when a distressing is found. Before acquiescing his duplicate check request for specific content, the user needs to take this content and his own constitutional rights as inputs.

The section II describes the related works about this project and section III and IV describes systemmodel and and proposed system finally section V and VI describes result and its conclusion.

II. RELATED WORK

Secure and well organized Proof of Storage with Deduplication:

Security notions such as Proof of Data Possession (PDP) and Proof of Retrievability (POR) have been bring for detecting that the data stored in the cloud has been tamper. On the other hand, an impluse of Proof of Ownership (POW) has also been proposed to alleviate the cloud server from storing multiple copies of the same data.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Proof of Data Storage with Deduplication :

Storage Server

Cloud provides storage service with relevant assurance protocol, by which the cloud storage clients can check the integrity of their data stored in the cloud.

Cloud storage clients

A client outsources its data to the cloud in a secure fashion, while allowing the cloud storage server to performance data deduplication operations[5].

Third Party Auditor

A client may allow a third party to check the probity of its data outsourced to the cloud.

Fast and Secure Laptop Backups with Encrypted Deduplication

Conventional backup solutions are not well suited to this environment and backup regimes are frequently inadequate. Each user only needs to record the keys for the root node. Typically, these would be stored independently on the backup system and encrypted with the user's personal key.

III. SYSTEM MODEL

Recent years have observe the trend of leveraging cloud-based services for large scale indebted cargo space, processing, and distribution. Security furthermore privacy are among top concerns for the public cloud environments. That is, every client calculates as per data key to encrypt the data that he intend to store in the cloud. As such, the data access is fare by the data owner.

3.1 System Model

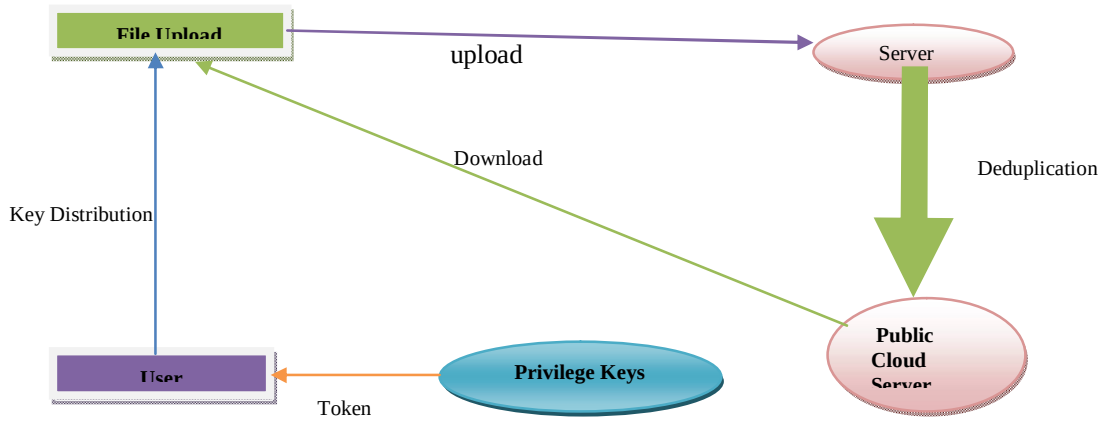

Fig 3.1 Deduplication checking process in cloud

Fig 3.1 represents user will upload the file contented in cloud server and then it verify for deduplication of the contented, if there is no replacement content it will upload in public cloud server. Then the desirable contented can be downloaded from cloud using the privilege key generated by cloud server for user.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

This paper introduces a current cryptographic method for secure Proof of Ownership (PoW), for humanizing data security in cloud storage systems, providing energetic sharing between users and ensuring efficient data deduplication[2]. On the other hand, it is used to ensure systematic access control in dynamic sharing scenarios. From the perception of cloud storage security.

IV. PROPOSED SYSTEM

4.1 Proof of Data Possession (PDP)

It allows a cloud buyer to verify the truthfulness of its data subcontracted to the cloud in a very efficient way. This is conceivable because it could be very resource-consuming to load a large data file from secondary storage to memory.

4.2 Proof of Retrievability (POR)

This notion was introduced by Juels and Kaliski. This explains the term “deduplication”. This concern was first introduced to the research community. Because straightforward deduplication is in danger to attacks Halevi proposed the notion called Proof of Ownership (POW)[1] as well as concrete constructions.

4.3 Target deduplication:

In recent years it’s be converted into clear that sponsorship up large amounts of data has a big impact on backup windows. Not only that there’s a mammoth cost involved in storing TBs or even PBs of backup data, and deduplication appliances have stepped into the fore. The procedure involves taking backup data, optimizing it through deduplication processes and store it on disk: “compressing” backup volume and saving money.

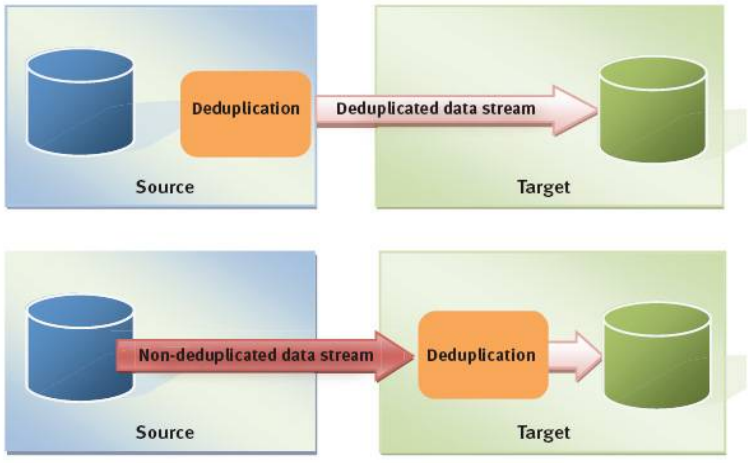

Fig 4.1 Target deduplication

Fig 4.1 represents that target deduplication is the taking away of redundancies from a backing spread as it passes through an machine sitting between the source and the backup target. The content that is uploaded by the source user is deduplicated then the target of cloud server contains deduplicated data stream otherwise target contains nonduplicated data stream.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Selected deduplication works very well and is still used in many environment. It's attractive because users only need to change the objective of the backup streams rather than tremendously changing their backup software configurations or policies. Target deduplication happens either on the fly, or as a post process. In one of its educational sessions, SNIA provides a view of target reduplication scenarios.

4.4 Global source-side deduplication:

Global source-side duplication remove redundancies from data before transmission to the backup target. The challenge is to ensure that the source (client) system is not go away down by deduplication software.Using global source-side deduplication across all patrons is central to limiting the unnecessary storage and relocate of duplicate backup data acquittal up server space and cutting down the time it takes to backup data.

Data is deduplicated across nodes, jobs and sites. Global deduplication goes past the limitations of network vendors. Its deduplication doesn't basically apply to the WAN replication cache it targets what is literally stored on disk. And as sponsorship data is globally deduplicated before it is transfer to the target backup server, only changes are sent over the network improving concert and tumbling bandwidth usage[4]. The entire process is protected with data store-intensity encryption and per-session passwords.

However, global orgin-side deduplication is built-into the backup server and require a new age bracket of data fortification Birthright backup solutions were not designed with deduce in mind so they can't really provide accommodation this breed of technology.

V. RESULTS

Proposed theory of tenable system was tested for its big data handling and deduplication efficiency. Here we tested deduplication good organization on various types of files.

	Deduplication Efficiency	Security achieved
Dropbox	84%	89%
Amazon	89%	93%
Proposed	91%	96%

Here we have implemented both target and source-side deduplication and obtained the efficiency of various organization of above 80%.And attained the security such that Dropbox achieved percentage of 89%,Amazon of about 93%.Any may achieve 96% percent in the proposed test bed experiment.

VI. CONCLUSION

Cloud computing has malformed into an of the essence perspective in today's. Cloud computing has conveyed with it a couple of challenge like security, stockpiling, booking etc. competence in Cloud prepare outlines a crucial part as the need of virtual space to store our expansive data has ended up over these years. As a proof of concept, implemented a prototype of our proposed authorized replacement check scheme and conduct test bed experiments on our prototype.

REFERENCES

[1] W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. InS. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium 2013.
[2] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl. A secure data deduplication scheme for cloud storage. In Technical Report, 2013.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

[3] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.
[4] J. Yuan and S. Yu .Secure and Efficient Proof of Storage with Deduplication.IACR Cryptology ePrint Archive, 2013:149, 2013.
[5] Nesrine Lauren France, fnesrine kaaniche. A Secure Client Side Deduplication Scheme in Cloud Storage Environments,2012.
[6] Jiawei Yuan, Shucheng Yu Department of Computer Science University of Arkansas at Little Rock. Secure and Constant Cost Public Cloud Storage Auditing with Deduplication.USA Email: sxyu1@ualr.edu 2012
[7] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491–500. ACM, 2011.
[8] Fabiano C. Botelho Gerais Belo Horizonte,br,Yoshiharu Kohayakawa Dept. of Computer Science Univ. of Sa˜o Paulo, Brazil . An Approach for Minimal Perfect Hash Functions for Very Large Databases yoshi@ime.usp.br.2011
[9] P. Anderson and Zhang . Fast and Secure Laptop Backups with Encrypted deduplication. In Proc. of USENIX LISA, 2010.
[10] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller. Secure data deduplication. In Proc. of StorageSS, 2008.