International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-7)

Research Article

July 2015

Hybrid Method by using Secured Privileged based De-Duplication in Cloud

[1]Vinod Jadhav, [2]Prof. Vinod Wadne
[1]PG Scholar, [2]Asst. Prof.
[1, 2] Computer Engg.Dept. Jspm's ICOER,Wagholi,
Savitribai Phule Pune University, Maharashtra, India

Abstract—

Cloud computing provide very cheap structure to take storage calculations. Many organization need to preserve and also operate huge amount of data.one of the most complicated problem of cloud computing is that management of increasing volume of data. For these the data de-duplication is used.
The data deduplication is data compression technique that improves utilization of storage by reducing the same data. Here we give data duplication method that is new data de-duplication method. Here we suggest confidentiality of de-duplication method here we introduced hybrid cloud method in these hybrid cloud we introduced two cloud one public cloud and one private cloud. A private cloud is an intermediate between public cloud and user. Private cloud gives set of private keys to user .we also support several deduplication methods.

Keywords— Hybrid Cloud, De-duplication

I. INTRODUCTION

Cloud storage is most useful storage in current years. Cloud computing is a method for giving information technology services where resources are accessed by web base tools and applications, instead of direct access to server. Cloud give extensible location independent and for data management in storage.to make data management in cloud de-duplication will be well known techniques and has attracted many more attraction currently. Data de-duplication is method that store only one instance of duplicated data and provide links to copy instead of storing actual copy of that data by storing only single copy of that data the de-duplication method useful to utilize storage space and also increases network bandwidth. In previous data de-duplication techniques each user use data encryption technique with their own keys because of these identical data copy is produced these gives different cipher text which gives data-deduplication impossible. So in our new model we are using the method which will take care of both security and extensibility.

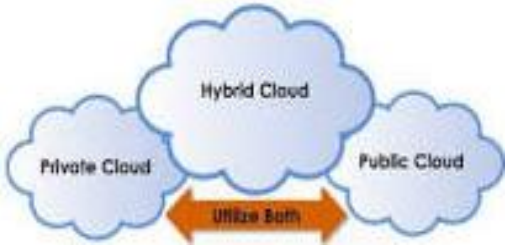

Figure 1 Authorized de-duplication model

Again old de-duplication technique does not support differential authorized duplication check. In this approach the user with different privileges on identical file also consider in duplicate check. If a file has two different user and both user have different privileges only one copy of file get stored..

II. MOTIVATION

The cloud storage became more focused method now days. Cloud provides very good way of storage with more efficient cost. One of the important problems of cloud is how to manage the everlasting increasing volume of data. These problem is sovled by data de-duplication method. There is some security issues of these motive us to manage these security issues in our new proposed model. And gives the authorized de-duplication method in cloud..

.

III. LITERATURE REVIVE

A Jan Stanek, Alessandro Sorniotti, Elli Androulaki, and Lukas Kencl [2]. Distinct the data with respect to their popularity for secure data deduplications the unfossed data is considered more important and gives the security to data and focused data that is used most of the user are considered less important and gives weak security concepts and good storage. A multilayer cryptographic mechanism is introduced

Such as convergent encryption and threshold encryption mechanism. The unfocussed files are led by the cover two layer whShai Halevi, Danny Harnik, Benny Pinkas, and Alexandra

Shulman-Peleg [3] the focused file are covered by single layer . Mainly focused on client side data deduplication. In client side data de-duplication if clients wants to upload any file on the server then it send the hash value of the data file to the server then server checks whether it is present or not if present it noticed to the client there is no need of storing the file otherwise it stores the file. but the problem is present at the client side data deuplication.in both the situation server highlight the client as the owner of the file and that stage there is no any kind of difference between server and client again any other person obtain the hash value can. To overcome such complicated situation proof of ownership is introduced. In this condition he is actual owner of such file without forwarding such file.in this approach the owner has to give identity the actual owner of the file without sending the proper file. A streaming protocol is introduced.

Mark W. Storer, Kevin , Darrell D. E. Long, Ethan L. Miller [4] mainly concerned with distinction between de-duplication and encryption. De-duplication can save only single file in case of encryption. Same file and same data decoded with two different keys result with different cipher text. That means same file and same content will be stored in the server. To overcome this problem a new approach introduced in which encryption keys are generated in consistent approach from block of data. there is two approach for data de-duplication, authenticated and anonymous .both method can be introduced to single server as well as distributed storage server approach. In this approach we used the convergent encryption technique and also in this approach plain text is also never sending to the server all the decode operation is done at the client side. Wee Keong Ng, Yonggang Wen, and Huafei Zhu [5] proposed the deduplication method for private data storage. Here the client has to prove his identity by proof of ownership protocol . a client who keep the private data proves the server thart he or she keeping the summery string of the file. Sven Bugiel, Stefan N□urnberger, Ahmad-Reza Sadeghi, and Thomas Schneider [6] mainly gives the outsourcing of the data . cloud computing gives more simple and effective approach for data storage. when data is outsource many security related issues and problems are comes inti picture such as malicious code running on the cloud. There may be a leakage of data. the primary requirement of cloud client is the confidentiality of the data. In proposed model the author introduced the twin cloud and commodity cloud. the working of the two cloud is different. The authorized cloud perform security operation such as encryption and commodity cloud perform time critical operation on the encrypted data. the client first of all make interaction with authorized cloud and then commodity cloud. John Douceur, Atul Adya, William J. Bolosky, Dan Simon and Marvin Theimer [7] make focus on distributed computing. To utlise the memory they used the convergent encryption technique in which the identical files are encrypted with different method still the different file is get stored. Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong [8] mentioned the peer-to-peer network application which store data effectively to the database and retrieval makes easy.

Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou [9] mention the efficient and very much reliable method of data de-duplication by using conversion encryption techniques. here theres is secure distribution of key management these convergent keys shares across multiple server.

Chun-Ho Ng and Patrick P. C. Lee [11] mentioned the de-duplication model which is distinct from another deduplication model. the deduplication is established for storage utilization it is also useful fo the fragmentation the deduplication remve duplicate data from old data not from new data.in thid deduplication if some duplicate data present then that old data is removed by the new data. Mihir Bellare, Sriram Keelveedhi, Thomas Ristenpart[13] mentioned a method in which a key is derived from message. This derived key is useful for the both encryption and decryption purpose. Here the symmetric encryption method use by which privacy and data integrity is maintained.

Jia Xu, Ee-Chien Chang, Jianying Zhou [15] have proposed the client-side data encryption method. They proposed the generalized encryption technique. The proposed approach gives more security against the outsider. Pasquale Puzio, Refik Molva, Melek □nen, Sergio Loureiro propose a system which introduce the confidentiality and block level de-duplication.thes system is based on convergent encryption technique. This convergent encryption technique gives us a key management method.thse method mainly focusses on cloud storage and storage, retrival

Table 1: Comparisons of Existing Model

Sr. No.	Methodology	Performance Evaluation			
		Security	Storage Efficiency	Computation Overhead	Bandwidth Consumption
1	Multi-layered cryptosystem [2]	Moderate	Moderate	High	Low (for popular data)
2	Merkle-hash tree [3]	Low	Moderate	Low	Low
3	Convergent encryption & SALAD [7]	Moderate	High	High	-
4	Ramp secret sharing scheme [9]	Moderate	High	Low	Low
5	Authenticated and Anonymous model [4]	Moderate	High	High	-
6	2-party computational model [5]	High	High	Moderate	-
7	Two cloud Architecture [6]	High	-	Low	Moderate
8	Client-Server Model [11]	-	Moderate	High	High
9	CE based MLE scheme [12]	High	High	High	High
10	Message lock encryption [14]	High	High	High	-
11	Client-side de-duplication scheme [15]	Moderate	Moderate	-	-
12	PCAD scheme polynomial based authentication tags and homomorphic linear authenticator [16]	High	High	Moderate	Low
13	Reverse De-duplication [19]	Moderate	Moderate	High	-
14	LiveDFS [20]	Moderate	Moderate	Moderate	-
15	POSD [30]	Moderate	Moderate	High	High
16	Hybrid cloud [29]	High	-	Low	-

Can Wang, Zhi-Guang Qin, Jing Peng Juan Wang proposes a best method for basic encryption is transformed from a single file to a chunk. The symmetric key is used to cipher text formation. These keys are generated by the chunk file content. K. Zhang, X. Zhou, Y. Chen, X. Wang, Y. Ruan proposes a hybrid cloud approach that support the data framework. These hybrid cloud introduced the public cloud and the private cloud . the sensitive information computation done by private cloud and non-sensitive information is present in the public cloud .

We have study different a approaches and comparative study among this approaches regarding data du-duplication in a cloud. We have also recognized their solution technique. We also checked the limitation of different techniques and also overcome some of problem regarding the limitation to improve the performance of the system in our new model. We introduced such a model tha model dis cribe the diffential privilege method of user with duplicate check. the owner of the file give authority to different user to acess the information from the file.in our new model we introduced the hybrid approach to protect the information. In these there are two cloud one is private cloud and other is public cloud.all the key distribution and duplicate information check is done by the private cloud only.in our newly introduced model system generated keys are used. The public cloud is only used for the data storage only.

IV. CONCLUSIONS

In these paper we have revive all the type of existing model for authorized de-duplication in cloud storage. By studying the existing system we introduced the new model that is hybrid cloud approach for authorized duplicate check in which we introduced the two cloud private cloud and public cloud.

ACKNOWLEDGMENT

I amvery much thanks to Prof. Vinod S Wadne for his valuable guidance.

We also thankful to our college administrative department, PG coordinator, HOD, Principal for availability of required infrastructure and their valuable support we would like to extend a genuine appreciation to my beloved friends and family members.

REFERENCES

[1] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serveraided encryption for deduplicated storage. In USENIX Security Symposium, 2013.

[2] P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted de-duplication. In Proc. of USENIX LISA, 2010.

[3] J. Li, X. Chen, M. Li, J. Li, P. Lee, andW. Lou. Secure de-duplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

[4] 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.

[5] J. Li, X. Chen, M. Li, J. Li, P. Lee, andW. Lou. Secure de-duplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

[6] C. Ng and P. Lee. Revdedup: A reverse de-duplication storage system optimized for reads to latest backups. In Proc. of APSYS, Apr 2013.

[7] C.-K Huang, L.-F Chien, and Y.-J Oyang, "Relevant Term Suggestion in Interactive Web Search Based on Contextual Information in Query Session Logs," J. Am. Soc. for Information science and Technology, vol. 54, no. 7, pp. 638-649, 2003.

[8] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011. W. K. Ng, Y. Wen, and H. Zhu. Private data de-duplication protocols in cloud storage. In S. Ossowski and

[9] P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing, pages 441–446. ACM, 2012.

[10] R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for de-duplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and communications Security, pages 81–82. ACM.

[11] S. Quinlan and S. Dorward. Venti: a new approach to archival storage. In Proc. USENIX FAST, Jan 2002.

[12] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui. A secure cloud backup system with assured deletion and version control. In 3rd International Workshop on Security in Cloud Computing, 2011.

[13] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. IEEE Computer, 29:38–47, Feb 1996.

[14] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl. A secure data de-duplication scheme for cloud storage. In TechnicalReport,2013.

