International Journal on Applications in Engineering and Technology
Volume 2: Issue 1: January 2016, pp 1-3 www.aetsjournal.com ISSN (Online) : 2455-0523

Security Enrichment of data in Web Cloud using DROPS

M. Muthu, R. Sachin Kumar Jaiswal, M.C. Sarathkumar, A. Sudhanram – Guided by L. Krishna Kumar

***Abstract*—**Cloud computing is a third party administrative control, here the data is outsourced so it gives rise to security concerns. Data compromise occur due to attacks or within the nodes itself. High security measures are needed to protect the data. In this paper, A Detach and Reproduction of Data in the Cloud for Excellent Performance and Security is proposed. In this methodology, a file is divided into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. In Division and Replication of data in cloud for Optimal Performance and Security (DROPS) methodology, it acquires more memory space and the data's won't be transact in a secure way and not in sequential order. To overcome these problem, an algorithm of Fragment and Shuffle -Drops (FS-Drops) is used along with Advanced Encryption Standard (AES).

***Keywords*—** Advanced Encryption Standard algorithm, Cloud computing, DROPS (Division and Replication of data in cloud for Optimal Performance and Security), Fragment and Shuffle, Security.

I. INTRODUCTION

Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings.

The prime disadvantage is security. To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor to audit the user's outsourced data when needed.

Therefore, in this paper, we collectively approach the issue of security and performance as a secure data replication problem. We present Detach and Reproduce of Data in the Cloud for Efficient Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the ocations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the FS-Algorithm. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. To further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/write requests. The selection of the nodes is performed in two phases. In the first phase, the nodes are selected for the initial placement of the fragments based on the centrality measures. In the second phase, the nodes are selected for replication. After duplication, it will shuffle the fragments. When user requested, it will retrieve the whole information in a sequential order.

II. DROPS METHODOLOGY

In the DROPS methodology, we propose not to store the entire file at a single node. The DROPS methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even a successful attack on the node leaks no significant information. The DROPS methodology uses controlled replication where each of the fragments is replicated only once in the cloud to improve the security. Although, the controlled replication does not improve the retrieval time to the level of full-scale replication, it significantly improves the security.

In the DROPS methodology, user sends the data file to cloud. The cloud manager system (a user facing server in the cloud that entertains user's requests) upon receiving the file performs: (a) fragmentation, (b) first cycle of nodes selection and stores one fragment over each of the selected node, and (c) second cycle of nodes selection for fragments replication. The cloud manager keeps record of the fragment placement and is assumed to be a secure entity. The fragmentation threshold of the data file is specified to be generated by the file owner. The file owner can specify the fragmentation threshold in terms of either percentage or the number and size of different fragments. The percentage fragmentation threshold, for instance, can dictate that each fragment will be of 5% size of the total size of the file. Alternatively, the owner may generate a separate file containing information about the fragment number and size, for instance, fragment 1 of size 5,000 Bytes, fragment 2 of size 8,749 Bytes. It is argued that the owner of the file is the best candidate to generate fragmentation threshold. The owner can best split the file such that each fragment does not contain significant amount of information as the owner is cognizant of all the facts

pertaining to the data. The default percentage fragmentation threshold can be made a part of the Service Level Agreement (SLA), if the user does not specify the fragmentation threshold while uploading the data file. We primarily focus the storage system security in this work with an assumption that the communication channel between user and the cloud

III. EXISTING SYSTEM

The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes (whether accidental or deliberate) must be prevented as discussed above, any weak entity can put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase an attacker's effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud. In this DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. And shuffling will be done by Graph T coloring algorithm. Here the fragments are scattered though the user cannot find the sequential order in this method but the retrieval time is very high. Moreover there is a chance of data loss and also data are not arranged in sequential order.

IV. PROPOSED SYSTEM

In this paper, we collectively approach the issue of security and performance as a secure data replication problem. We present Detaching and reproducing of Data in the Cloud for Excellent Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. In addition we added two algorithms are used first one is FS-Drops (Fragment and Snuffle -Drops) Which will fragment a file into 4 pieces and shuffled And store in different server So in future some Server is not available are Hacked we can get back our original data from remaining Server. The second is to forward the data to others in secure manner. So the user request to forward the data from cloud to others mean the server generates a key for a specific file and provided to the cloud user. The random function used to generate a key. The keys are shared by the sender and receiver. By using the secret key the receiver can fetch data from the cloud securely.

V.FRAGMENTATION

In fragmentation, we are splitting the file in to small fragments. Once the file is split into fragments, this concept selects the cloud nodes for fragment placement. The selection is made by keeping an equal focus on both security and performance in terms of the access time. The process is repeated until all of the fragments are placed at the nodes. Partial Replication represents the fragment placement methodology. Mainly we focus on the storage system security in this work. As stated above, the probability of a successful coordinated attack is extremely minute.

VI. CONCLUSION AND FUTURE WORK

We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file. The performance of the DROPS methodology was compared with full-scale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance, resulted in increased security level of data accompanied by a slight performance drop. Currently with the DROPS methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The aforesaid future work will save the time and resources utilized in downloading, updating, and uploading the file again. Moreover, the implications of TCP incest over the DROPS methodology need to be studied that is relevant to distributed data storage and access.

VII. REFERENCES

[1] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Quantitative comparisons of the state of the art data center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.

[2] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

[3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.

[4] Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.

[5] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol.9, No. 2, 2011, pp. 50-57.

[6] W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[7] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, "An analysis of security issues for cloud

computing," Journal of Internet Services and Applications, Vol. 4, No. 1,2013, pp. 1-13.
[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.
[9] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference on System Sciences (HICSS), 2011, pp. 1-10.
[10] A. Juels and A. Opera, "New approaches to security and availability for cloud data," Communications of the ACM, Vol. 56, No. 2, 2013, pp. 64-73.
[11] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant Filesystems," University of Ioannina, Greece, Technical Report No.DCS2013-1, 2013.
[12] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.
[13] S. U. Khan, and I. Ahmad, "Comparison and analysis of ten static heuristics-based Internet data replication techniques," Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008,pp. 113-136.
[14] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards Secure Mobile Cloud Computing: A Survey," Future Generation Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.
[15] A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, The Journal of Supercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706.
[16] T. Loukopoulos and I. Ahmad, "Static and adaptive distributed data replication using genetic algorithms," Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp. 1270-1285.
[17] A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003, pp. 885-896.
[18] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, "On the placement of web server replicas," In Proceedings of INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1587-1596, 2001.