



A Survey on Data Security Using Data Partitioning and Replication Technique

Alkute Pranali, Auti Harshada, Shirsath Aarti, Tathe Prajakta, Prof. Agale D. B.

B.E Student, Dept. of Computer Engineering, SCSMCOE, Nepti, Ahmednagar, Maharashtra, India

Asst. Professor, Dept. of Computer Engineering, SCSMCOE, Nepti, Ahmednagar, Maharashtra, India

ABSTRACT: Outsourcing data to another authoritative control will be done in distributed system, ascend to security concern. This data trade off happens because of assaults by different types of users and nodes inside the cloud system. Hence, high security efforts to establish safety are required to secure information inside the cloud storage. On the other side, the given security procedure should likewise consider the advancement of the information recovery time. Paper will be, In this paper we propose Division and Replication of Data in the Cloud storage for Optimal Performance and Security (DROPS) that will be collectively approaches the security and performance issues. In the DROPS procedure, as per user input file partition into sections, and reproduce the divided information on the cloud storage nodes. Each of the node store just a small byte part of that file information record that guarantees that even in the event of a fruitful assault, no important data is uncovered to the assailant. More thinking like, the nodes putting away the section is isolated with separation by the method for diagrams T-shading to restrict an assailant of speculating the areas of the section. Then, the DROPS System does not depend upon customer cryptographic system will be the information security; in this way alleviating the arrangement of computationally costly approaches. We show the demonstration that the likelihood to find and bargain the greater part of the nodes putting away the section of a solitary recording is to the great degree low. We likewise analyze the run of the DROPS system with different plans. The more elevated amount of security with a execution overhead was watches.

KEYWORDS: cloud storage security, file fragmentation, text file replication, high performance.

I. INTRODUCTION

Security is the most important aspects among those the wide-spread adoption eclipse of cloud computing. Cloud security problem supported due to core technology implementation as like virtual machine (VM) escape or session riding, etc. The service offerings by cloud as SQL injection or less authentication system and cloud characteristics like information recovery vulnerability and Internet protocol vulnerability, data storages, etc. To secure cloud all the participating entities must be provides security. In the cloud security of the assets does not completely depend on an individual's security measures because an any given system with one or more units, the highest level of systems security is equal to level of the weak entity and so the neighbouring entities may provide an opportunity to an attacker. The off-line data storage cloud utility requires users to move data in clouds virtualized and shared environment that may result in various security procedures. Pooling and elasticity of cloud storage allows the physical resources to be the shared maximum users. Shared resources may be reassigned to other users at same instance of time that may result in data compromise through data recovery techniques. The information similarly, cross-tenant virtualizes network accessing may also compromise data safety and data integrity. Inapplicable media sanitization can also hack customer's private data. The Unauthorized information/data accessing by user and processes must be prevented. This system is useful to user for successfully store the fragrant. In such criteria, the security mechanism must be the substantially increasing an attacker's/hacker effort to retrieve a reasonable amount of data even after the successful attack in the cloud storage. The sufficient amount of loss information present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially fragments user text files into small part and replicates them at strategic locations within the cloud.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

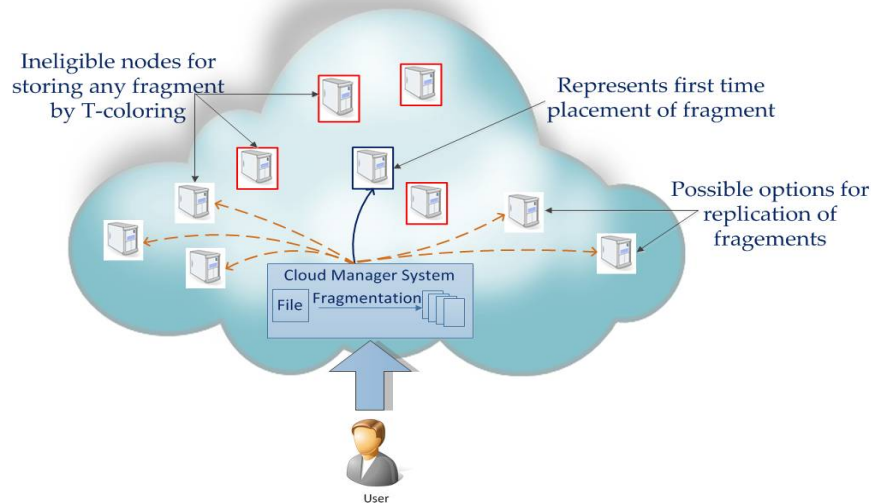


Fig: DROPS methods

II. RELATED WORK

Data Fragmentation:

Data fragmentation means divides the file, fragments and replicate store on each node present into the cloud storage. A successful intrusion into a single node may have not available, not only for data and applications on the victim node, but also for the other nodes. If an hacker /attacker's uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very weak. Let will be the consider cloud as M nodes and input file with z number of fragments. Let s be the number of successful attack's on distinct nodes, such that $s \geq z$. The probability that s number of victim nodes contain all of the z sites storing the file fragments (represented by $P(s,z)$) is given as:

DROPS

System Model:

In this project algorithms are used to fragments placement and fragments replication. A cloud that consists of a M nodes, each node with its own capacity. Let S_i represents the name of i -th node and s_i denotes total storage capacity of S_i . Communication time between S_i and S_j is the total time of all of the links within a selected path from S_i to S_j represent by $c(i, j)$. We consider N number of file fragments such that O_k denotes k -th fragments of a file while o_k represents the size of k -th fragments. P_k denote the primary nodes that storage the primary copy of O_k , replication scheme for O_k denoted by R_k is also store at P_k and Whenever there is an update in not as an independent documents. Please do not revise any of the current designations O_k , the updated version is sent to P_k that broadcasts the updated version to all of the nodes in R_k . Let $col(S_i)$ store the value of assigned color to S_i . The $col(S_i)$ can have one out of two values, namely, open-color and close-color. The value open-color represents that the node is available for storing the for file fragment. The value close-color shows that the node cannot store the file fragment. The set T is used restrict the nodes selection to those nodes that are at hop-distances not from to T . In the DROPS methodology, we propose not to store the entire files at the single node. The DROPS methodology fragments the files and makes use to the cloud for replications. The fragments are distributing such that no node in to the cloud holds more than single fragment, so that even a successful attack on the node leaks no significant information. In DROPS methodology, user sends the data file to cloud storage. The cloud administrative system receive the file status: (a) fragmentation of file, (b) first cycle of nodes selection and stores one fragment over each of the selecting node, (c) second cycle of nodes selection for fragments replication on to the replicated node. The cloud administrative keeps record of the fragment placement and is assumed will be secure entity.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

III. PROPOSED SYSTEM

In drops paper, we collectively rules the issues of security and performance as a securethe file. DROPS: Division and Replication of Data in the Cloud storage for Optimal Performance and Security that fragments user files into small part and replicates them at strategic locations withinto the cloud storage nodes. The division of a file into fragments is performing based on the giving input criteria such that as the individual fragments do not contain any meaningful data. Each of thecloud node(we use the term node to represent storage capacity, physical, and the virtual machines) contains will be distinct fragment to increase the more data security on cloud.

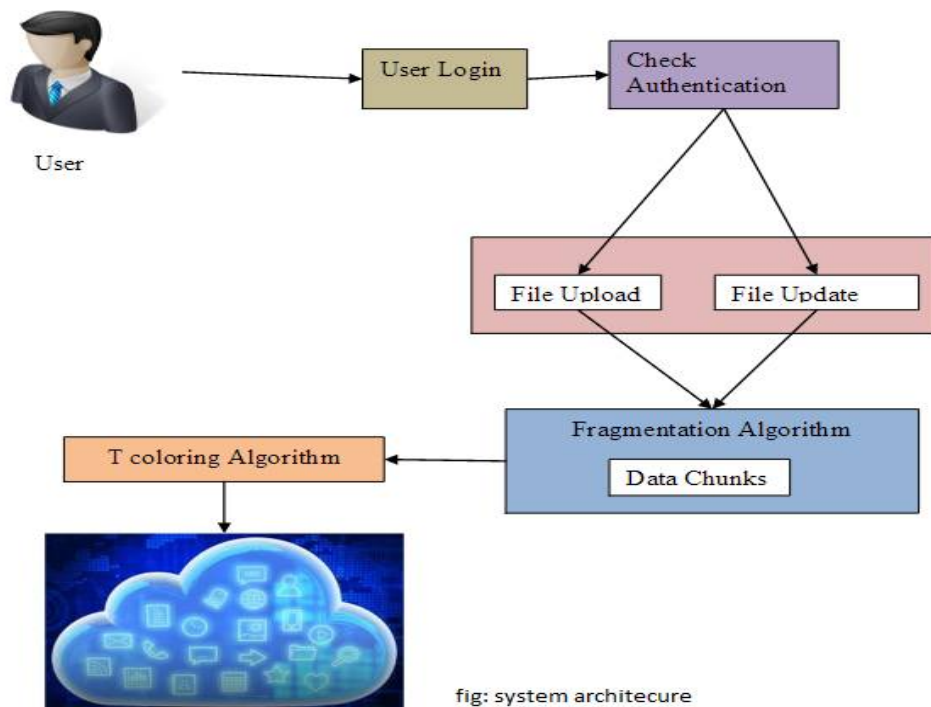


fig: system architecture

IV. CONCLUSION AND FUTURE WORK

In this paper it is the proposed that DROPS methodology is a distributed storage security conspire that by and large manages the security and execution as recovery time. The information record was divided and the parts are scattered over different nodes. The nodes were isolating by method for T-shading. The discontinuity and dispersal guaranteed that no noteworthy data was reachable by the enemy if there should be an occurrence of a fruitful assault. No node in to the cloud put away more than a solitary part of the same documents. The executing of the DROPS system was contrasting and will be full-scale of the fragments and replication strategies. As now with the DROPS approach, a user needs to download the reports, redesign the substance, and transfer it once more. It is important to build up a programming upgrade instrument that can recognize and overhaul the required sections just. User can uploading files, updates, modify, delete, etc. It gives the information related to the (DROPS) Division and replication of data in cloud Storage for optimal performance and security.

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.



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 9, September 2016

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. Fernandez-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.