ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Method to Optimize Performance and Security by Division and Replication of Data in Cloud

Suravarapu Jaya Sai Rajitha
M.Tech Student
Department of CSE,
ASR College of Engineering,
(Affiliated to JNTUK, Kakinada)
Tetali, Tanuku,
West Godavari Dt, Andhra Pradesh.

A.Girija
Assistant Professor,
Department of CSE,
ASR College of Engineering,
(Affiliated to JNTUK, Kakinada)
Tetali, Tanuku
West Godavari Dt, Andhra Pradesh.

ABSTRACT:

Outsourcing information to an outsider authoritative control, as is done in distributed computing, offers ascend to security concerns. The information trade off may happen because of assaults by different clients and hubs inside of the cloud. Hence, high efforts to establish safety are required to secure information inside of the cloud. On the other hand, the utilized security procedure should likewise consider the advancement of the information recovery time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that all in all methodologies the security and execution issues. In the DROPS procedure, we partition a record into sections, and reproduce the divided information over the cloud hubs. Each of the hubs stores just a itary part of a specific information record that guarantees that even in the event of a fruitful assault, no important data is uncovered to the assailant. Additionally, the hubs putting away the sections are isolated with certain separation by method for diagram T-shading to restrict an assailant of speculating the areas of the sections. Moreover, the DROPS procedure does not depend on the customary cryptographic procedures for the information security; in this way alleviating the arrangement of computationally costly approaches. We demonstrate that the likelihood to find and bargain the greater part of the hubs putting away the sections of a solitary record is to a great degree low. We likewise analyze the execution of the DROPS system with ten different plans. The more elevated amount of security with slight execution overhead was watched.

Key words: ***Centrality, cloud security, fragmentation, replication, performance***

INTRODUCTION

Security is one of the most crucial aspects among those the wide-spread adoption of cloud computing [14, 19]. Cloud security issues sustained due to the core technology implementation as like virtual machine (VM) escape or session riding, etc. The service offerings by cloud as structured query language injection or weak authentication schemes and cloud characteristics like data recovery vulnerability and Internet protocol vulnerability, etc.)

To secure cloud all of the participating entities must be secure. In a cloud the security of the assets does not solely depend on an individual's security measures because In any given system with multiple units, the highest level of the systems security is equal to the security level of the weakest entity [12] [5] and so the neighboring entities may provide an opportunity to an attacker .The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. The Pooling and elasticity of a cloud allows the physical resources to be shared among many users [22]. Shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies [2].The data [9]. Similarly, cross-tenant virtualized

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

network access may also compromise data privacy and integrity. Improper media sanitization can also leak customer's private data [5].

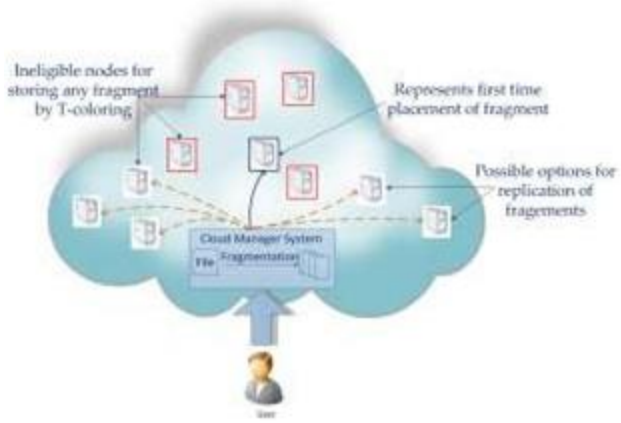

Figure1: DROP Method

The Unauthorized data access by users and processes must be prevented [4]. An 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. The probable amount of loss (as a result of data leakage) present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.

For each of the cloud nodes 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 locations of other fragments within the cloud. 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 Second phase, the nodes are selected for replication. The working of the DROPS methodology is shown as a high-level work flow and comparative techniques to the DROPS methodology. The various implemented replication strategies are: (a) A-star based searching technique for data replication problem (DRPA-star) (b) Weighted A-star (WA-star), (c) A-star, (d) Suboptimal A-star1 (SA1) (e) suboptimal A-star2 (SA2), (f) Suboptimal A-star3 (SA3) (g) Local Min-Min, (h) Global Min-Min, (i) Greedy algorithm, and (j) Genetic Replication Algorithm (GRA).Here three Data Center Network (DCN) architectures, namely: (a) Three tier, (b) Fat tree, and (c) D Cell. We use the aforesaid architectures because they constitute the modern cloud infrastructures and the DROPS methodology is proposed to work for the cloud computing paradigm.

Contributions in this paper are as follows:

The proposed scheme fragments and replicates the data file over cloud nodes.

The proposed DROPS scheme ensures that even in the case of a successful attack. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations. Here ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security

Data Fragmentation:

A successful intrusion into a single node may have severe consequences, not only for data and applications on the victim node, but also for the other nodes. if an attacker is uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very low.

Let us consider a cloud with M nodes and a filewith z number of fragments. Let s be the number of successful intrusions on distinct nodes, such that s>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:

A cloud that consists of M nodes, each with its own storage capacity. Let Si represents the name of i -th node and si denotes total storage capacity of Si

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Communication time between Si and Sj is the total time of all of the links within a selected path from Si to Sj represented by c(i, j) .

We consider N number of file fragments such that Ok denotes k -th fragment of a file while ok represents the size of k-th fragment. Pk denote the primary node that stores the primary copy of Ok, replication scheme for Ok denoted by Rk is also stored at Pk and Whenever there is an update in not as an independent document. Please do not revise any of the current designations Ok , the updated version is sent to Pk that broadcasts the updated version to all of the nodes in Rk .

Let colSi store the value of assigned color to Si . The colSi 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 file fragment. The value close color shows that the node cannot store the file fragment The set T is used to restrict the node selection to those nodes that are at hop-distances not belonging to T. 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 single fragment, so that even a successful attack on the node leaks no significant information.

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.

Then compared the results of the DROPS methodology with fine-grained replication strategies, namely:
(a) DRPA-star,
(b) WA-star,
(c) Aʟ -star,
(d) SA1,
(e) SA2,
(f) SA3,
(g) Local Min-Min,
(h) Global Min- Min,
(i) Greedy algorithm, and
(j) Genetic Replication Algorithm (GRA).

The DRPA-star is a data replication algorithm based on the A-star best-first search algorithm. The DRPA-star starts from the null solution that is called a root node.

CONCLUSION

The proposed 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.

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.