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 10, October 2016

A Survey on Data Security Using Data Partitioning and Replication Techniques

Nirmale Pooja S., Kore Pranjali P. , Pratape Pradnya P., Patil Mayur H.

B. E Students, Dept. of Computer Engineering, JSPM'S ICOER, Wagholi, Pune, Maharashtra, India

ABSTRACT: Outsourcing data to beanother authoritative controlwill be done in distributed system,ascend to security concern. This data trade off happen 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 be proposes Division and Replication of Data in the Cloudstorage for Optimal Performance and Security (DROPS) that will be collectivel1y approaches the security and performance issues. In the DROPS procedure, as per user input file partitioninto 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 uncover 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 customercryptographicsystemwill 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 [1] [2]. In the cloud security of the assets does not completely depend on an individual's security measures because 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 cloudstorage allows the physical resourcesto 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 informationsimilarly, cross-tenant virtualizes network accessing may also compromise data Safety and data integrity [3]. 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.

DOI: 10.15680/IJIRCCE.2016. 0410157

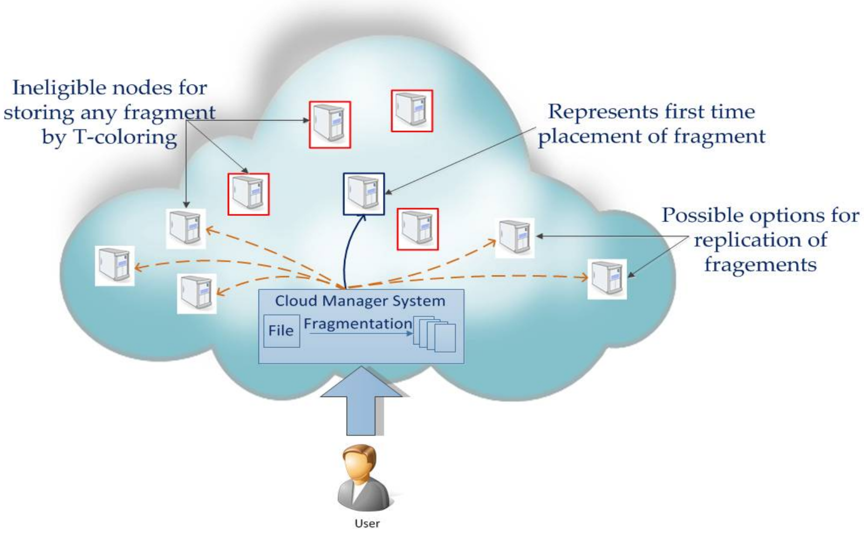
Ineligible nodes for storing any fragment by T-coloring
Represents first time placement of fragment
Possible options for replication of fragements
Cloud Manager System
File
Fragmentation
User

Fig:1. DROPS methods

II. LITERATURE SURVEY

To ensuring high reliability in data centres, distributing the power and resource cooling, storage capacity are purveyed. The operational cost will be reduced by using the replicated data in cloud node. In cloud, resources will be leads to a congestion in service purveying. This will saves the energy consumption. Therefore data replication, which fetches data near to data customer seen as auspiciousresolution. Bandwidth and network detain are diminished by the replication. Here replication algorithm is using for gaining the performance as well as energy efficiency. The performance can be measured using availability, responsetime and data centre congestion and Failures and loss occurred in data is analyzed bythe replication cost model. Replicated data will be supported by the distributed system.Internet plays a vital role in every one’s life for accessing and rapid dispersal of data. One possible solution is replicating few of objects at various places is for decreasing network traffic. Then we need to decide where to replicate and whatkind of datato replicate, Allocation, consistency and fault tolerance are the three main issues of replication.In this paper, Genetic Replication algorithm (GRA) [2] solves the problems of read/write demands and quality is obtained by comparing it with greedy method (Simple Replication Algorithm). Regrettably, when read/write demands are continuously changing, The static genetic algorithm (GA) is not useful because it involves high running time. To overcome that problem, the author presents an adaptive genetic replication algorithm (AGRA) and it takes as input for current replica distribution and using knowledge we can determines a new one, when changes are happened. Morenumber of requests can be handled in popular web servers for providing good quality services to customers. So that by using replication techniques, it ensure contents of from up-todate, information can be retrieved in fast, load can be

A. 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 onthe victim node, but also for the other nodes [4]. If an hacker /attacker’s uncertain about the locations of the fragments, theprobability of finding fragments on all of the nodes is very weak.Let will be the consider cloud as M nodes and input filewith z number of fragments. Let s be the number of successfulattack’s on distinct nodes, such that s>=z . The probability that s number of victim nodes contain all of the z sitesstoring the file fragments (represented by P(s,z)) is given as:

B. 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 [5]. Let Si represents the name of i -th node andsi denotes total storage capacity of Si Communication time between Si and Sj is the total time of all of the linkswithin a selected path from Si to Sj represent by c(i, j).We consider N number of file fragments such that Ok denotes k -th fragments of a file while ok represents the sizeof k-th fragments. Pk denote the primary nodes that storage the primary copy of Ok, replication scheme for Okdenoted by Rk is also store at Pk and Whenever there is an update in not as an independent documents. Pleasedo not revise any of the current designations OK, the updated version is sent to Pk that broadcasts the updatedversion 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-colorand close-color. The value open-color represents that the node is available for storing the for file fragment. The valueclose-color shows that the node cannot store the file fragment. The set T is used restrict the nodes selection tothose nodes that are at hop-distances not from to T. In the DROPS methodology, we propose not to store theentire 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 asuccessful attack on the node leaks no significant information.In DROPS methodology, user sends the data file to cloudstorage. The cloud administrative systemreceive the file status: (a) fragmentation of file, (b) first cycle ofnodes selection and stores one fragment over each of the selecting node,(c) second cycle of nodes selectionfor fragments replication on to the replicated node [7]. The cloud administrative keeps record of the fragment placement and is assumed will besecure entity.

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.

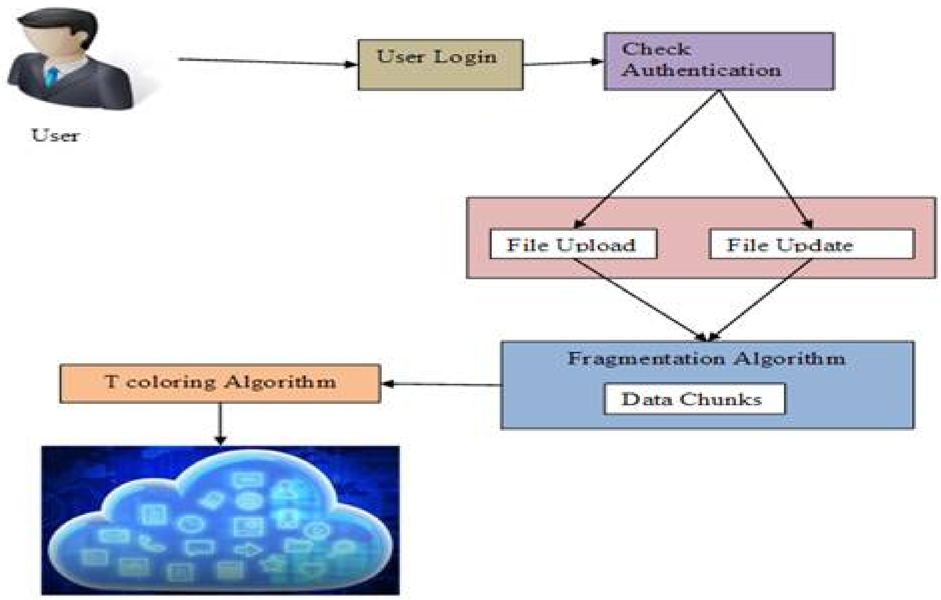

Fig.2 system Architecture

Above figure shows the user module uploads the text file on the cloudstorage. Then the admin modules fragments the file using algorithms and store oneach node. Presented a technique to ensure the integrity, freshness, and availability ofdata in a cloud. The data migration to the cloud is performed by the Iris file system.A gateway application is designed and employed in the organization that ensures theintegrity and freshness of the data using a Merkle tree. The file blocks, MAC codes,and version numbers are stored at various levels of the tree. The proposed techniquein heavily depends on the users employed scheme for data confidentiality. Moreover,the probable amount of loss in case of data tempering as a result of intrusion oraccess by other VMs cannot be decreased. Our proposed strategy does not dependon the traditional cryptographic techniques for data security. Moreover, the DROPSmethodology does not store the whole file on a single node to avoid compromise ofall of the data in case of successful attack on the node. The authors in approachedthe virtualized and multi-tenancy related issues in the cloud storage by utilizing theconsolidated storage and native access control. The Dike authorization architectureis proposed that combines the native access control and the tenant name space isolation.The proposed system is designed and works for object based file systems.

However, the leakage of critical information in case of improper sanitization andmalicious VM is not handled. The DROPS methodology handles the leakage of criticalinformation by fragmenting data file and using multiple nodes to store a singlefile.

IV. CONCLUSION

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 a rise 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 thefragments 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 theinformation 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.
3. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,“Energy-efficient data replication incloud 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.