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 11, November 2016

Improving Performance and Security by Using Division and Replication of Data in Cloud

Swapnil Jagade[1], Nilesh Ghare[2], Mukul Gosavi[3], Sunil Lahane[4], Prof. Kavitajadhav[5]

Student, Siddhant College of Engineering, Pune, Savitribai Phule Pune University, Pune India[1,2,3,4]

Siddhant College of Engineering, Pune, Savitribai Phule Pune University, Pune India.[5]

ABSTRACT: Outsourcing data to an untouchable legitimate control, as is done in disseminated processing, offers rise to security concerns. The information bargain may happen because of assaults by pernicious clients and nodes inside the cloud.Along these lines, high security frameworks are required to ensure information inside the cloud. Nevertheless, the used security strategy ought to similarly consider the headway of the data recuperation time.In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues.In the DROPS methodology, we partition a document into sections, and afterward reproduce the divided information over the cloud nodes. Each of the nodes contains just a solitary section of a specific information record that guarantees that even if there should be an occurrence of a fruitful assault, no any important data is unveil to the assailant.Besides, the nodes putting away the sections are isolated with certain separation by means of graph T-coloring to banish from an assailant of speculating the areas of the parts. In addition, the DROPS methodology does not depend on the traditional cryptographic techniques for the data security; along these lines soothing the arrangement of computationally exorbitant strategies. We demonstrate that the consequence to find and trade off the greater part of the nodes putting away the sections of a solitary document is to a great degree low.We likewise contrast the execution of our procedure and other condition of-workmanship plans. The more elevated amount of security with slight execution overhead was watched.

KEYWORDS: Cloud Computing,Centrality, Cloud Security, Fragmentation,Replication, Performance, Internet Protocol Vulnerability.

I. INTRODUCTION

The cloud computing worldview has transformed the utilization and administration of the data innovation system.Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The previously mentioned qualities of cloud computing make it an obvious contender for organizations, associations, and individual clients for appropriation. Be that as it may, the advantages of least cost, insignificant administration (from a clients viewpoint), and more noteworthy flexibility accompany expanded security concerns. Security is a standout amongst the most critical angles among those restricting the far reaching reception of cloud computing.Cloud security issues may stem due to the core technologies implementation (virtual machine (VM) escape, session riding, etc.), cloud service presenting (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.). For a cloud to be secure, the greater part of the taking an interest elements must be secure. In any given framework with numerous units, the most elevated amount of the frameworks security is equivalent to the security level of the weakest element. Along these lines, in a cloud, the security of the benefits does not totally rely on upon an individual's security measure. The neighboring elements may give a chance to an assailant to reroute the client's safeguards.

II. LITERATURE SURVEY

Juels et al., [2] exhibited a strategy to ensure the trustworthiness, curiosity, and accessibility of information in a cloud. The information movement to the cloud is performed by the Iris file system. A gateway application is designed and employed in the organization that ensures the integrity and novelty of the data using a Merkle tree. The file blocks, MAC codes, and version numbers are kept at various levels of the tree. Moreover, the probable amount of loss in case of data tempering as a result of intrusion or access by other VMs cannot be decreased.

G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, [3] presented the virtualized and multi-tenancy related issues in the cloud storage by using the joined stockpiling and nearby get to control. The Dike authorization architecture is proposed that combines the local access control and the tenant name space isolation.

D. Zissis and D. Lekkas, [5] introduced the utilization of a trusted outsider for giving security benefits in the cloud. The authors used the public key infrastructure (PKI) to increase the level of trust in the authentication, integrity (unity), and confidentiality of data and the communication between the involved parties. The keys are generated and managed by the certification authorities. At the client level, the utilization of aura evidence gadgets, such as smart cards was proposed for the storage of the keys.

D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, [6] proposed Energy-efficient data replication in cloud computing datacenters.A central database (Central DB), placed in the wide-area network, provide all the data required by the cloud applications. To speed up the access and reduce latency, each data center hosts a local database, called datacenter database (Datacenter DB). It is utilized to copy the most as often as possible utilized information things from the central database. Each rack hosts at least one server capable of running local rack-level database (Rack DB), which is used for replication (duplication) of data from the datacenter database.

Sabrina De Capitani di Vimercati1, Robert F. Erbacher2, [7] presented Encryption and fragmentation for data confidentiality in the cloud which perform fragmentation of file. Fragmentation consists in splitting the attributes of a relation R producing different vertical views (fragments) in such a way that these views placed at external providers do not disregard secretly necessities (neither directly nor indirectly). Instinctively, fragmentation protects the sensitive association represented by an association constraint c when the attributes in c do not appear all in the same (publicly available) fragment, and fragments cannot be joined by non authorized users.

M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, [10] presented a secure and optimal placement of data objects in a distributed system is presented. An encryption key is splitted into n shares and distributed on different sites within the network. The division of a key into n shares is carried out through the (k, n) threshold secret sharing scheme. The network is divided into clusters. The number of duplicas and their placement is determined through heuristics. A primary site is selected in each of the clusters that distribute the replicas within the cluster.

Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei Dai, [11] proposed CHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability which integrates two key functions desired.The first is picking a few reasonable mists and a precise excess methodology to store information with minimized financial cost and ensured accessibility. The second is accelerating a move procedure to re-distribute data according to the variations of data access pattern and pricing of clouds.

Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, [12] proposed Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage. To resolve the regeneration problem of failed authenticators in the absence of data owners, they introduce a proxy, which is chartered to regenerate the authenticators, into the traditional public auditing system model. Moreover, they design a shocker public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can fully release data owners from online burden. In addition, the system randomize the encode coefficients with a pseudorandom function to jelly data privacy.

Shristi Sharma, ShreyaJaiswal, Priyanka Sharma, Prof. Deepshikha Patel, Prof. Sweta Gupta, [13] are proposed An Approach for File Splitting and Merging. File Splitter is a program which does not require installation and can be used to split files to multiple chunks as well as to merge multiple chunks into a single file. File Splitter is software which is utilized to split the user characterizing record as per the user indicating size. It is very difficult to transfer one big file from one end to another via any media like internet or small storage like Floppy, Pen drive, CD etc. This software helps to resolve this problem. The split portions of file may keep together some temporary information to denote the number of split part and total number of parts etc. This idea is used to split big files to small pieces for transferring purpose, uploading etc. In the destination side, these parts of file can be collectedto form the original source file. Splitting process is mainly aiming in the area of file transposing from one end to another.

III. EXISTING SYSTEM APPROACH

In existing system information dependability, information accessibility, and reaction time are managed information replication techniques. Be that as it may, putting away imitations information over various nodes expands the assault surface for that specific information. For instance, putting away m copies of a record in a cloud rather than one copy builds the likelihood of a node holding document to be picked as assault sufferer, from 1/n to m/n where n is the aggregate number of nodes. Existing framework was not accomplishing legitimate security.

Disadvantage:

1) A key element deciding the throughput of a cloud that stores information is the information recovery time.
2) In vast scale frameworks, the issues of information unwavering quality, information accessibility, and reaction time are managed information replication systems.

3) However, putting copies information over various nodes builds the assault surface for that specific information.
4) Affected on security and execution.

IV. PROPOSED SYSTEM APPROACH

We propose a new idea Division and Replication of Data in Cloud thatjointly approaches the security and performance issues in terms of retrieval time. The proposed scheme ensures that even in the case of a successful attack, no meaningful information is disclosedto the attacker. We don't rely on upon conventional cryptographic strategies for information security. The non-cryptographic nature of the proposed conspire makes it speedier to play out the required operations (arrangement and recovery) on the information. We ensure a controlled replication of the document parts, where each of the pieces is duplicated once with the end goal of enhanced security. A cloud storage security conspire mutually manages the security and execution regarding recovery time.
Advantage:

1) Improve security.
2) Improve performance.
3) No any information is revealed to the attacker.
4) No load on single node of cloud.
5) Numbers of fragments are decided according to owner’s choice.

V. PROPOSED ARCHITECTURE

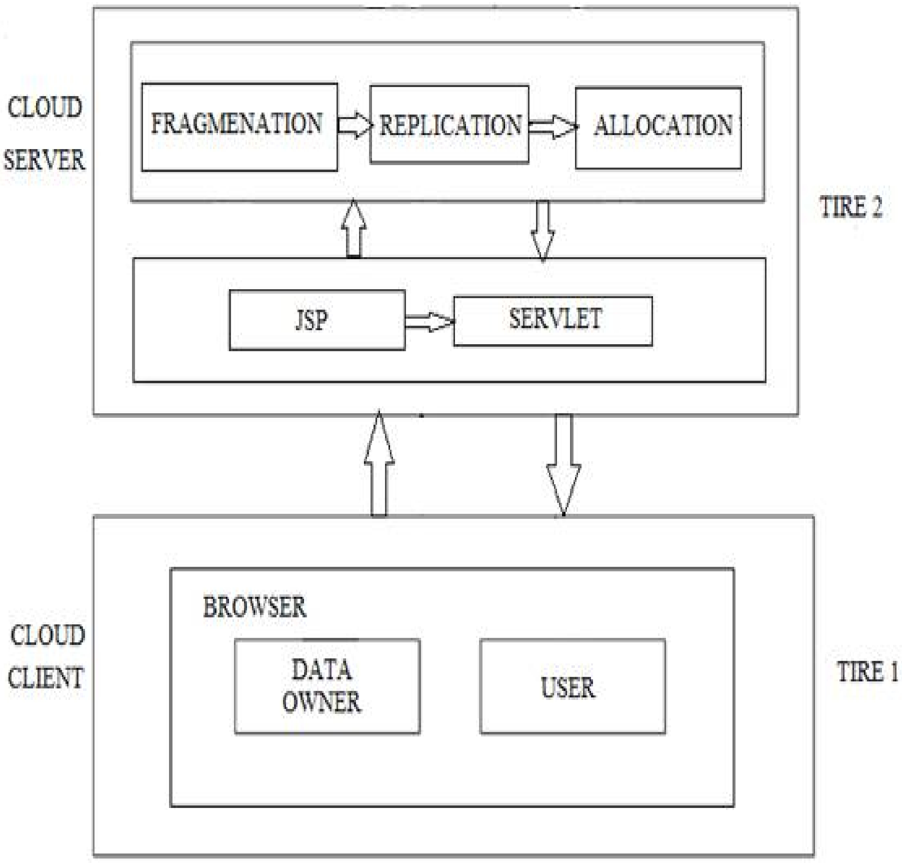

Fig No 01. System Architecture

DOI: 10.15680/IJIRCCE.2016. 0411141

VI. MODULES

1) Cloud Client:-

Cloud client should be Data owner or Data user.

- Data Owner:-
  Data owner is responsible for uploading file on cloud as well as view files uploaded by him or others. Data owner has information about the placed fragment and its replicas with their node numbers in cloud.
- Data User:-
  Data user is the one who is responsible for downloading files or view files uploaded by others. To download file from cloud he has to be authenticated user otherwise he will be considered as attacker.
- Admin:-
  Admin is an authorized person who has rights to validate authorized data owner and user. He is also responsible for allocation of block and maintains information and authentication.

2) Cloud Server:-

- Fragmentation:-
  This approach is used for fragmenting the file for security purpose at sever side. This approach runs the Fragmentation algorithm. It has file as input and produces the file fragments as output.

- Replication:-
  This approach creates replicas (duplicate copy) of fragments. These replicas are useful when one of fragment is corrupted by attacker then to provide file for user admin replaces its replica at that place and combine all fragments and send file to authenticated user or data owner. To make replicas of file fragments this approach runs replication algorithm which takes input as fragments and produces its replicas as output.
- Allocation:-
  After the file is spitted and replicas are generated then we have to allocate that fragments at cloud server for storing data. While storing or allocating that fragments we have consider security issues. So we are using T-Coloring Graph concept for placing fragments at different nodes on cloud server. This approach runs Fragment allocation algorithm which takes input as fragments and produces the output as fragments allocated with node numbers.

VII. CONCLUSION

We proposed the new methodology, Division and Replication of Data in Cloud thatjointly approaches the security and performance issues in terms of retrieval time. The information record was divided and the parts are scattered over different nodes. The nodes were isolated by method forT-coloring. The fracture and dispersal ensure that no huge data was reachable by an enemy if there should arise an occurrence of a fruitful assault. No node in the cloud put away more than a solitary part of a similar document.The performance of our Division and Replication of Data in Cloudmethodology was differentiatedwith full-scale replication techniques. The aftereffects of the reenactments disclosed that the synchronous concentrate on the security and execution brought about expanded security level of information joined by a slight execution drop.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, Vol. 28, No. 3,2012, pp. 583-592.

[6] 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.

[7] Sabrina De Capitani di Vimercati1, Robert F. Erbacher2, “Encryption and fragmentation for data confidentiality in the cloud”.

[8] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, “Secure overlay cloud storage with access control and assured deletion,” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, Nov. 2012, pp. 903-916.

[9] “Division and Replication of Data in Cloud for Optimal Performance and Security” azhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan.

[10] M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, “On the optimal placement of secure data objects over Internet,” In Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, pp. 14-14, 2005.

[11] Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei Dai, “CHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability”. IEEE Transactions on Cloud Computing, Volume: 3March2015.

[12] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, “Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage”. IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 7, July 2015.

[13] Shristi Sharma, ShreyaJaiswal, Priyanka Sharma, Prof. Deepshikha Patel, Prof. Sweta Gupta, “An Approach for File Splitting and Merging” Lecturer, Department of IT Technocrats Institute of Technology, Bhopal.