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 Paper on Drops: Division and Replication of Data in Cloud for Optimal Performance and Security

Nidhi Jain[1], Prof. Archana jadhav[2]

M. E Student, Dept. of Computer Engineering, Alard College of Engineering and Management, SavitribaiPhule Pune University, Pune, India [1]

Dept. of Computer Engineering, Alard College of Engineering and Management, SavitribaiPhule Pune University, Pune, India [2]

ABSTRACT: Outsourcing information to an outsider authoritative control, as is done in distributed computing, offers ascend to security concerns.The data compromise may occur due to attacks by malicious users and nodes within the cloud.Therefore, high security systems are required to protect data within the cloud.Be that as it may, the utilized security technique 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 collectively approaches the security and performance issues.In the DROPS methodology, we divide a file into fragments, and then replicate the fragmented data over the cloud nodes.Each of the nodes contains only a single fragment of a particular data file that ensures that even in case of a successful attack, no any meaningful information is disclose to the attacker.Furthermore, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to bar from an attacker of guessing the locations of the fragments.Moreover, the DROPS methodology does not depend on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally costly methodologies.We show that the eventuality to locate and compromise all of the nodes storing the fragments of a single file is extremely low.We also compare the performance of the DROPS methodology with ten other state-of-art schemes. The higher level of security with slight performance overhead was observed.

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

I. INTRODUCTION

The cloud computing paradigm has reformed the usage and management of the information technology framework. Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The aforementioned characteristics of cloud computing make it a conspicuous candidate for businesses, organizations, and individual users for adoption.However, the benefits of minimum cost, negligible management (from a users perspective), and greater elasticity come with increased security concerns. Security is one of the most crucial aspects among those forbiddingthe wide-spread adoption 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, all of the participating entities must be secure.In any given system with multiple units, the highest level of the systems security is equal to the security level of the weakest entity. Therefore, in a cloud, the security of the assets does not completely depend on an individual's security measure. The neighboring entities may provide an opportunity to an attacker to detour the user's defenses.

DOI: 10.15680/IJIRCCE.2016. 0410174

II. LITERATURE SURVEY

Juels et al., [2] presented a technique to make sure the integrity, novelty, and availability of data 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 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 utilizing the combinedstorage and local access 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] presented the use of a trusted third party for providing security services 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 user level, the use of disposition proof devices, 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 used to duplicate the most frequently used data items 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 stored at external providers do not violate secretly requirements (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 choosing several suitable clouds and an accurate redundancy strategy to store data with minimized economic cost and guaranteed availability. The second is precipitatinga transition process 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 used to split the user definingfile according to the user specifying size. It is very hard to transfer one big file from one end to another through any media like internet or small storage like Floppy, Pen drive, CD etc. This software helps to solve this problem. The split portions of file may carry 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 jointed to form the original source file. Splitting process is mainly aiming in the area of file transferring from one end to another.

III. EXISTING SYSTEM APPROACH

In existing system data reliability, data availability, and response time are dealt with data replication strategies.However, storing replicas data over a number of nodes increases the attack surface for that particular data.For example, storing m replicas of a file in a cloud instead of one replica increases the probability of a node holding file to be chosen as attack sufferer, from 1/n to m/nwhere nis the total number of nodes. Existing system was not achieving proper security.

Disadvantage:

1) A key factor determining the throughput of a cloud that stores data is the data retrieval time.
2) In large-scale systems, the problems of data reliability, data availability, and response time are dealt with data replication strategies.
3) However, placing replicas data over a number of nodes increases the attack surface for that particular data.
4) Affected on security and performance.

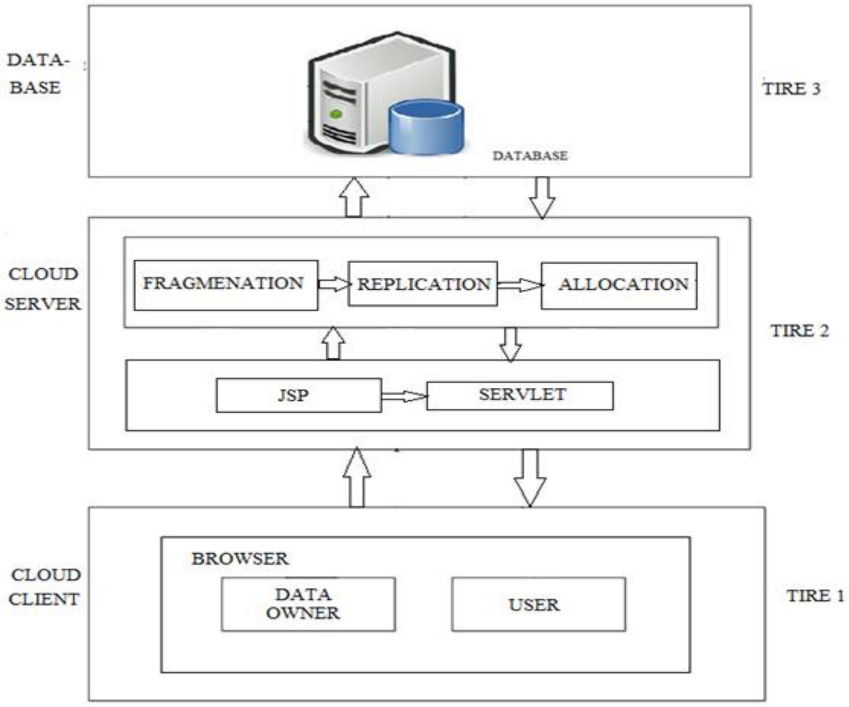
IV. PROPOSED SYSTEM APPROACH

We propose a new idea called DROPS(Division and Replication of Data in Cloud for Optimal Performance and Security) that jointly approaches the security and performance issues. The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is disclosedto the attacker. We do not depend on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. We make sure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security. A cloud storage security scheme jointly deals with thesecurity and performance in terms of retrieval 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



System Architecture

DOI: 10.15680/IJIRCCE.2016. 0410174

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.

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.

3) 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.

VII. CONCLUSION

We proposed the DROPS methodology, a cloud storage security scheme that jointly deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are scatteredover multiple nodes. The nodes were separated by means of T-coloring. The fragmentation and dispersal make sure that no significant information was obtainable by an antagonist 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 differentiatedwith full-scale replication techniques. The results of the simulations divulgedthat the simultaneous focus on the security and performance resulted in increased security level of data accompanied by a slight performance 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.