International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

Harshal Dilip Patil[1], M. D. Ingle[2]

[1]Department Computer Engineering, Jayawantrao Sawant College of Engineering, HadapsarPune-28, Savitribai Phule Pune University, Pune, India

[2]Professor, Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar Pune-28, SavitribaiPhule Pune University, Pune, India

Abstract: ***The issues related to security and performance overcomes by the Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS). In cloud computing, the data is stored on third party space gives rise to security concerns. The user and node within cloud may compromise the data. Therefore, to protect data within the cloud high security measures are required. Divide a file into fragments, and replicate the fragmented data over the cloud nodes is done in DROPS methodology. Only a single fragment of a particular data file can be stored by each of the nodes that ensure that no meaningful information is revealed to the attacker even in case of a successful attack.***

Keywords: Centrality, cloud security, fragmentation, replication, performance

1. Introduction

Distributed computing's prominent adaptability accompany expanded security concerns. Security is a standout amongst the most pivotal perspectives among those forbidding the fare chin reception of distributed computing.

The majority of the taking part substances must be secure for a cloud to be secure. The largest amount of the systems security is equivalent to the security level of the weakest element in any given framework with numerous units. In this way, in a cloud to establish safety, the security of the benefits does not exclusively rely on upon an individual's efforts.

To move information in cloud's virtualized and shared environment that may bring about different security concerns, the offsite information stockpiling cloud utility obliges clients. The physical assets to be shared among numerous clients may be pertimed by Pooling and flexibility of a cloud. In this paper as a safe information replication issue, we by and large approach the issue of security andexecution.

We introduce Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS). It parts client records into pieces and repeats them at vital Distributed computing. In any case, the security concern get expanded by the advantages of minimal effort, insignificant administration (from a client's point of view), and more prominent adaptability accompany. Security is a standout amongst the most pivotal perspectives among those forbidding the fare chin reception of distributed computing.

The majority of the taking part substances must be secure for a cloud to be secure. The largest amount of the systems security is equivalent to the security level of the weakest element in any given framework with numerous units. In this way, in a cloud, the security of the benefits does not exclusively rely on upon an individual's efforts to establish safety. To move information in cloud's virtualized and shared environment that may bring about different security concerns,the offsite information stockpiling cloud utility obliges clients. The physical assets to be shared among numerous clients get permitted by Pooling and flexibility of a cloud. In this paper the issue of security and execution as a safe information replication issue, we by and large approach.

2. Related Work

J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, had presented the Cloud computing growth due to its core technology raises the security issue. So, to achieve the security as well as performance by using three techniques, Graphical Password Authentication, Fragmentation and Replication, this system provides a better solution. Nowadays, the use of the Graphical Password Authentication increases. This is because as compared to alphanumeric method, it is very easy to remember and secure. Fragmentation used to secure data from single point disaster. In failure situations, Replication can be useful for maintaining availability, reliability and performance. But due to extreme use of bandwidth the extra replication can also result in high storage cost or drops in systems overall performance. So, here controlled replication is used. The time and work on some attacks will get saved in the future work.[1]

S. U. Khan, and I. Ahmad Cloud computing, while quickly evolving, can offer IT departments a powerful choice for delivering application program. Cloud computing promises scalable, on-need resources; flexible, self-serve deployment; lower TCO; faster time to market; and a mass of service option. It can legion your entire substructure, be a part of your substructure, or simply serve a single application. No matter how far into the swarm you are, or if it is a public, private, or cross cloud , F5 solution can help make your cloud infrastructure or deployment more secure, reliable, and resilient. IT administrators can isolate constellation and

direction for fine -grained control over admission to cloud computing infrastructure and can isolate application traffic for improved protection of application data that uses shared resources.[2]

D.Boru, D.Kliazovich, F.Granelli, P.Bouvry, and A. Y. Zomaya, Divided a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file. It ensures that even in case of a successful attack, the attacker fail to get meaningful information.[3]

T. Loukopoulos and I. Ahmadto improve the resource limitation of mobile devices, mobile users may utilize cloud-computational and storage services. The processing and storage capacity of mobile devices, the migration of confidential information on untrusted cloud raises security and privacy issues get improved by the utilization of the cloud services improves. [4]

K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya analyzed robustness of the state-of-the-art DCNs. The paper's major contributions are: 1) It presented multilayered graph modeling of various DCNs; 2) It studied the classical robustness metrics considering various failure scenarios to perform a comparative analysis; 3) It presented the inadequacy of the classical network robustness metrics to appropriately evaluate the DCN robustness; and 4) It proposed new procedures to quantify the DCN robustness. Therefore, for the future DCN robustness research, we believe that this study will lay a firm foundation.[5]

K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez a very wide study had been reviewed which signifies threats with service and deployment models of cloud. this study is presented so as to effectively refine the crude security issues under various areas of cloud in order to comprehend these threats. This study also aims at revealing different security threats which were under the cloud models as well as network concerns to stagnate the threats within cloud, facilitating researchers, cloud providers and end users for noteworthy analysis of threats.[6]

3. Proposed Work

Our paper describes a technique The DROPS methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The future work will save the time and resources utilized in downloading, updating, and uploading the file again. Moreover, the implications of TCP in cast over the DROPS methodology need to be studied that is relevant to distributed data storage and access. We develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme divides the file in fragments and replicates the data file over cloud nodes. The proposed DROPS scheme ensures that no meaningful information is revealed to the attacker even in the case of a successful attack. We do not rely on traditional cryptographic techniques for data security. To perform the required operations (placement and retrieval) on the data, the non-cryptographic nature of the proposed scheme makes it faster. We ensure a controlled replication of the file fragments, Where each of the fragments is replicated Only once for the purpose of improved security.

4. Architectural View

The architecture diagram of the system shown below helps us to understand the system.

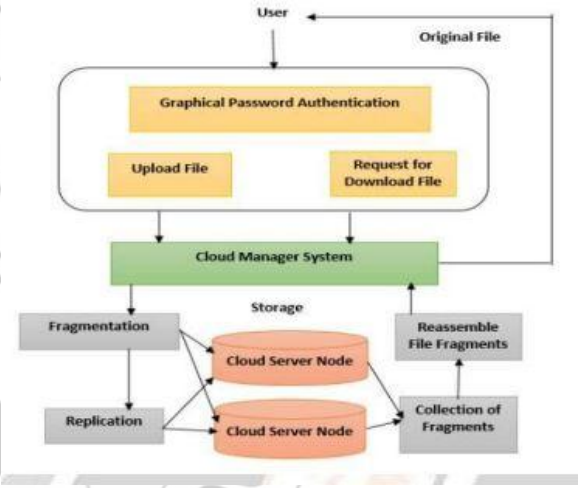

Figure 1: System Architecture

In this paper, as a secure data replication problem we collectively approach the issue of security and performance. We present DROPS that fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security

Sr No.	Paper	Technique	Advantages	Disadvantage
1	On the characterization of the structural robustness of data center networks	DCN Models	Network (or also referred to as topology) robustness is the ability of the network to deliver the expected level of performance	High level of network robustness leads to higher cost
2	Energy-efficient data replication in cloud computing datacenters	Bandwidth Model, data replication technique	data replication technique for cloud computing data centers which optimizes energy consumption, network bandwidth and communication delay	untested implementation
3	New approaches to security and availability for cloud data	Error correcting technique	Secure cloud data by ensuring the range of protection	Rarely rely primarily on externally managed source
4	Dike: Virtualization-aware Access Control for Multitenant File systems	externally apply techniques of encryption, hashing and auditing to achieve end-to-end confidentiality, integrity and freshness	natively support multitenant access control	possibly shared system files in read-only mode
5	Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing	Light weight algorithm which generates automatic dynamic credentials.	Enhances the security of user credentials.	unstable connectivity and introduce several security issues
6	A survey of mobile cloud computing application Models	location algorithm based on the location history of a smartphone	Done trust management to support mobile cloud computing is a totally unexplored area	issue for building MCC applications
7	Secure overlay cloud storage with access control and assured deletion	AES algorithm with the cipher block chaining	provide assured deletion for files	will create another security issue.
8	Addressing cloud computing security Issues	client/server deployment models	ability to address vulnerabilities recognized in traditional IS	critical issue for the success of information systems

5. Conclusion

Cloud computing growth raises the security concern due to its core technology. So, this system provides a better solution to achieve the security as well as performance by using three techniques, Graphical Password Authentication, Fragmentation and Replication. Nowadays, the use of the Graphical Password Authentication increases because it is very easy to remember and secure as compared to alphanumeric method. Fragmentation used to protect data from single point disaster. Replication can be useful for maintaining availability, reliability and performance in failure situations. But the extra replication can also result in high storage cost or drops in systems overall performance due to extreme use of bandwidth. So, here controlled replication is used. The future work will saves the time and work on some attacks. Matching Based Over-lapping approach reduces the computational load of alignment by reducing the pattern sequence into a smaller set of overlapped subsequences. Furthermore, the detection and the update processes can be parallel with no loss of accuracy.

References

[1] J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, “Selecting the right data distribution scheme for a survivable storage system,” Carnegie Mellon University, Technical Report CMU-CS-01-120, May 2001.

[2] S. U. Khan, and I. Ahmad, “Comparison and analysis of ten static heuristics-based Internet data replication techniques,” Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008, pp. 113-136.

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

[4] Loukopoulos and I. Ahmad, “Static and adaptive distributed data replication using genetic algorithms,” Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp. 1270-1285.

[5] 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.

[6] 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.

Author Profile

Mrs. Harshal D. Patil is currently pursuing M.E (Computer) from Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India. SavitribaiPhule PuneUniversity, Pune, Maharashtra, India -411007. She received her B.E (Computer) Degree from SSVPS B.S.D College of Engineering, Dhule, India. North Maharashtra University,Jalgaon, Maharashtra, India - 424001. Her area of interest is Cloud Computing.

Prof. Madhav D. Ingle received his M Tech. (Computer) Degree from Dr. BabasahebAmbedkar Technological University, Lonere, Dist. Raigad-402103, Maharashtra, India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India. He is currently working as M.E coordinator and Asso. Prof. (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. SavitribaiPhule Pune University,Pune, Maharashtra, India - 411007. His area of interest is network security and WSN.