Frontiers in Health Informatics
ISSN-Online: 2676-7104

www.healthinformaticsjournal.com

2024; Vol 13: Issue 7

Open Access

Optimizing Cloud Performance and Security Through Data Partitioning and Replication

Soham Sunil Kulkarni[1],Suket Gakhar[2],Anant Kumar[3],Vishesh Nirwal[4]

[1]Computer Science, University of California, IRVINE. grepsoham@gmail.com

[2]Master of Technology, Computer Science and Engineering, Kurukshetra University, Kurukshetra. suket.gakhar@gmail.com

[3]M. Tech, Computer Science & Engineering, Manipal Institute of Technology, Manipal. anant.bhagath@gmail.com

[4]Master of Engineering, Computer Technology and Applications, University of Delhi, Delhi. Nirwal.v@gmail.com

Cite this paper as: Soham Sunil Kulkarni,Suket Gakhar,Anant Kumar,Vishesh Nirwal (2024) Optimizing Cloud Performance and Security Through Data Partitioning and Replication. *Frontiers in Health Informatics, 13* (7), 80-89

ABSTRACT: As occurs with cloud computing, re-appropriating information to an outsider managerial power raises security issues. Different clients and clouds hubs may assault the information split the difference. Therefore, they are likely to maintain great efforts in the safety of cloud information. In any case, the artistic creations of the working security plan needs to recollect time efficiency of information recovery too. In this artworks, we educate Division and Replication regarding the "Information withinside the Cloud for Ideal Execution and Security (DROPS)" that, as one purposes the wellbeing and execution issues. In DROPS approach, we segment a document and mirror the disheveled information over the cloud communities. To perceive this, each center draws in with handiest an unmarried fragment of a given information record, withinside the event that an assault is a hit no imperative information is transferred to the aggressor. Furthermore, chart T-shading separates the hubs stocking the parts with a distance so that an adversary cannot anticipate the locations of the segments. Also, using DROPS approach keeps the framework free from computationally costly techniques because of not utilizing the traditional cryptographic methods for the information security. We show that there is very minimal opportunity to find and think twice about hub keeping portions of a solitary document. We additionally assess the exhibition of the DROPS procedure among ten elective methodologies. There was noticed a more significant level of safety with a little exhibition above.

"Keywords: *—Centrality, cloud security, fragmentation, replication, performance."*

1. INTRODUCTION

The key and insisting viewpoint of cloud computing has influenced the use and support of the data innovation foundation. When requested self administrations, obligatory organisation arrives at, resources pooling, versatility and approximated administrations explain cloud computing. The parts of distributed computing talked about above make it a fascinating possibility for use by associations, clubs, and confidential clients. From the perspective of the client, however, in each case the advantage of low cost, low overhead – that is flexibility — also brings with it greater vulnerability. One of the main variables among those forbading the overall acknowledgment of cloud computing is security. This should emerge from the order of the center advancement which incorporate VM getting away, gathering utilizing and the preferences, cloud the board commitments which incorporate mixing based question language, slight approval plans and the preferences and in the end the ones ascending from cloud characteristics comprehensive of measurements rebuilding delicacy, Web meeting fragility and the rest. Cloud cannot be secure unless each of the complex components are also secure. An irregular edges two or three gadgets has maximal confirmation of se wellbeing is indistinguishable from the security of the significantly less consistent component. Thus in a cloud, wellbeing of the resources is moored in a bonus than individual security drills. The encompassing elements could allow an aggressor an opportunity to move beyond the client securities. Hence, information security has changed as clients of cloud outer information stockpiling utilities should move their information to the cloud's virtualized shared environment.The pooling and adaptability of the cloud implies that various clients share a typical pool of actual assets. Moreover, eventually of time the common assets could be moved to another client that could think twice about through information recuperation strategies. Besides, a multi-inhabitant virtualized climate could create a virtual machine to get past the restrictions of virtual machine monitor (VMM). To get admittance to unlawful information, the getting away from virtual machine might upset other VMs. Cross-inhabitant virtualized network access could accordingly risk information uprightness and protection. Unseemly media disinfecting could possibly uncover private data of buyers.

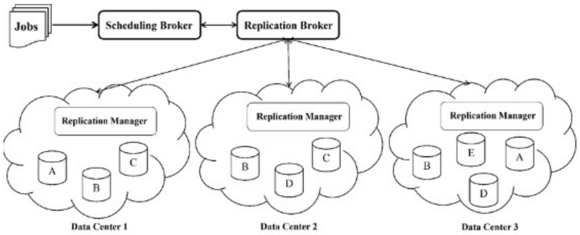


Fig.1: Example figure

The data shipped off a public cloud must be locked. Whether unexpected or purposeful, unapproved information access by others and frameworks must be halted. Any powerless element can so imperil the entire cloud, as was at that point referenced. Under such a circumstance, the security framework needs to essentially raise the work of an aggressor to recuperate an OK volume of information in any event, following an effective cloud entrance. Moreover, the reasonable misfortune coming about because of information spilling must be monitored.

2. LITERATURE REVIEW

“On the characterization of the structural robustness of data center networks:”

The "Information and Communication Technology (ICT)" industry depends fundamentally upon server ranches as both compositional and valuable block of distributed computing. From agribusiness to nuclear science, splendid systems to clinical consideration, web crawlers for research reason, and Data and Limit and Assessment reason, distributed computing is generally utilized in many fields. Coordinating the communicational spinal string of a server ranch, a "Data Center Network (DCN)" concludes the show obstructions for cloud designing. To meet the vital “Quality of Service (QoS) level and fulfill Administration Level Understanding (SLA)”, the DCN should areas of strength for be disappointments and vulnerability. We examine in this work the strength of the best in class DCNs. The fundamental assertions are (a) we provide a multiple perspective diagram demonstrating of various DCNs; (b) we investigate the primitive power metrics based on distinct disappointment scenario to perform a like examination; (c) We show how the customary boss energy measures really do now never again adequately hold onto the DCN strength; and (d) we explain new strategy to appraise the goodness of the DCN meticulousness. Not much careful examination on the DCN power exists at the present time. Hence, we imagine that the future DCN heartiness exploration will have areas of strength for a thanks to this work.

“Energy-efficient data replication in cloud computing datacenters:”

Arising as a worldview with figuring assets accessible as a help across an organization is cloud computing. For the overwhelming majority cloud applications, correspondence assets habitually address an obstruction in help provisioningThusly, considered a setup permits information replication to bring information (e.g., datasets) nearer to information purchasers (e.g., cloud applications), permitting command over network inactivity and transfer speed use. In this work we explore information replication in server farms of cloud computing. Unlike other strategies described in the writing, we take into account energy per productivity as well as framework data transfer capacity use regardless of the higher Quality of Service (QoS) accompanying lower correspondence delay. The obtained assessment of vast scope reproductions contributes to identifying compromises in execution and energy productivity, as well as indicating the design of subsequent information replication arrangements.

Intrusion tolerance in cloud computing systems:

An interference open minded appropriated framework is one that is intended to guarantee that assaults on any piece of the framework are liberated from dread, honesty, and classification. For appropriated frameworks, this methodology is reasonable in light of the fact that circulation permits some level of separation of parts, so goes after just permit actual admittance to parts of the framework. For instance, an interference lenient check and approval server can be applied to different untrusted has, supporting a bound together security framework oversaw by untrusted (yet not helpful) faculty. Engineers propose how different appropriated framework parts can be intended to safeguard against these assaults. A genuine model of a disseminated record server was really made and carried out as one of the subtasks of the Delta 4 task of the European ESPRIT program.

Understanding cloud computing vulnerabilities:

The ongoing conversation of the security of distributed computing is an educated appraisal exertion for two primary reasons. In the first place, as is normal in numerous conversations of chance, general terms, for example, "risk," "peril," and "weakness" are frequently utilized reciprocally, no matter what their particular importance. Second, none of the worries raised are intended for distributed computing. Breaking down what cloud computing means for each chance part assists us with having a right information on the security issue "delta". One critical component connects with weaknesses: cloud computing presents new weaknesses and builds the importance of a few notable ones. Here the makers give a security-explicit cloud reference configuration, grasp 4 side effects and side effects of cloud-explicit shortcomings, and convey cases of cloud-explicit shortcomings for each underlying part.

Frequency assignment: Theory and applications:

In this work we give a hypothesis associating the base request way to deal with recurrence task to the ordinary one and present this technique. Potentially more engaging than the traditional strategy is this new one. Task issues are demonstrated by us as both recurrence distance restricted and recurrence compelled optimizable issues. Assuming distance division is utilized to diminish impedance, one ought to stay away from the recurrence restricted method. Recurrence distance restricted issues are for the most part related with a restricted class of charts known as circle diagrams. We describe two conjectures about chromatic number and prove they are related to many recurrence task issues with summed up diagram shading issues. We place several recurrence task issues on the basis of the ‘execution time effectiveness’ of calculations that may be devised to solve them by such equivalencies and recent findings regarding the complexity of diagram shading. We discuss how We go over utilizes for huge worldwide issues and pinpoint regions requiring more exploration.

3. IMPLEMENTATION

Juels et al. given a strategy to ensure cloud information accessibility, respectability, and newness. The Iris record framework drives the information relocation to the cloud. Utilizing a Merkle tree, a door application is created and utilized in the organization ensuring information respectability and newness. At a few levels of the tree are kept the record blocks, Macintosh codes, and variant numbers.

Using the blended storing and neighborhood gain section to influence, G. Kappeset. al. managed the virtualized and multi-inhabitance related inconveniences withinside the distributed storage. Proposed is a Dam endorsement design uniting occupant call region isolation with neighborhood gain passage to influence.

DISADVANTAGES:

- ❖ In instances of broken disinfection and threatening virtual machines, the spilling of significant data isn't tended to.
- ❖ These sorts of frameworks don't safeguard the information documents against altering and misfortune welcomed on by virtualization and multi-tenure.
- ❖ The information documents are handled as one single record and are not divided.

In this work, each the wellbeing and execution parts of a covered measurements replication bother are tended to. We present Division and Replication of Information withinside the Cloud for Ideal Execution and Security (DROPS); invigorated through the legal executive framework, parting and dividing clients' documents then recreating them at key variables withinside the cloud.

A record is isolated into segments according to decided client guidelines so much that each part comes up short on immense information. Each cloud center — we call them center points to portray register, limit, physical, and virtual machines — has an exceptional segment to help data security.

We make a framework for re-appropriating information thinking about execution as well as security. The proposed structure portions the records record over cloud centers.

Advantages:

- ❖ The proposed DROPS structure guarantees that even in the event of an effective assault, huge measure of information isn't presented to the aggressor.
- ❖ We don't depend on conventional encryption procedures for data security. Non-encryptors in our suggested structure accelerate the significant undertakings of coordinating and recuperating data.
- ❖ It plays out a sort of controlled duplication of record segments, for example each part is duplicated just a single time for further developed security.

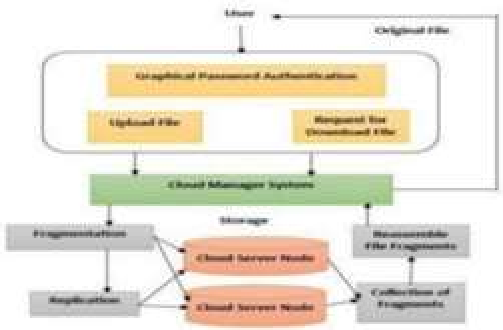


Fig.2: System model

MODULES:

- ❖ “System Construction”
- ❖ “Data Fragmentation”
- ❖ “Centrality”
- ❖ “DROPS”

MODULES DESCSRIPTION:

System Construction:

- ❖ ❖ In the principal module, we propose an arrangement for a system designing module to break down and execute dividing and replication of data on cloud for ideal activity and security, and propose a functional engineering idea called DROPS. We build Client and Cloud elements for this point. In Client element, a client could refresh transferred Document blocks by transferring another Record.

- Our framework model tends to two sorts of substances: clients and cloud servers. Unique client is the person who transferred each document to the cloud server; resulting client is the person who exhibited the responsibility for record however didn't actually present the document to the cloud server.
- The cloud first and foremost investigate login approval of clients withinside the Cloud substance; thusly, it awards authorization for approved clients and clients figures are kept in blocks.
- We have portrayed a plan to assess and upgrade the ,current methodology and looked at the asymptotic portrayal of the plan ,with tantamount plans, ,where ,n, is the quantity of blocks, ,b, is the quantity of blocks tried and ,|m|, is the size of the block. ,Besides, contrasted with different methodologies with lower security ,affirmations, our methodology shows preferable asymptotic conduct over ,different methodologies.

Data Fragmentation

- This module assists us with building the information discontinuity. Compromising a solitary record will require the work to get to only one hubA typical methodology is to separated individual pieces of a data informational collection and store them in various centers to diminish the possibilities of the data being compromised. A fruitful interruption on one or scarcely any hubs will just concede admittance to a subset of conceivably immaterial information.
- Moreover, on the off chance that the aggressor doesn't have the foggiest idea about the area of the parts, the likelihood of finding them at every hub is very low.The given information document is consequently parted and distributed in the cloud so the programmer can't find the data.In a cloud framework, the possibilities of an assailant having the option to gather a lot of information are significantly decreased. In any case, putting each section once in the framework will abbreviate the information recovery time.
- Pieces can be repeated such that brings recovery times down to a level that doesn't raise the previously mentioned probability, consequently further developing the information recovery times.

Centrality

- The proportion of a hub's general significance in an organization is given by its centrality in a chart. Upgraded recovery times in replication help to accentuate the centrality estimations.
- Centrality gauges incorporate closeness centrality, degree centrality, betweenness centrality, flightiness centrality and eigenvector centrality.Since this study utilizes the three organization centralities referenced above, we essentially think about closeness, betweenness and capriciousness centrality.

DROPS

- Utilizing the DROPS approach, separates the document and imitations it utilizing the cloud. The sections are conveyed to such an extent that every hub in a cloud holds more than one part, in this manner guaranteeing that even an effective From the strategy of DROPS loses no significant information. security is still advanced through controlled replication where every part is replicated solely once in the cloud. Be that as it may, this gives a critical improvement in security, as recuperation times with restricted replication are not similar to those of full replication.
- According to the DROPS approach, the client transfers an information document to a cloud.. Once the document is acquired, the cloud director framework a client confronting server in the cloud that meets client demand carries out discontinuity, first pattern of hubs determination and stores one segment over every one of the chose hub, and second pattern of hubs determination for parts replication. Being considered as a safe substance, the cloud supervisor captures part position.

4. METHODOLOGY

Algorithms:

Cloud computing:

Cloud computing is the use of equipment and programming based PC assets provided as a help across an organization, generally the Web.

The name gets from the continuous reflection of the convoluted framework found in framework graphs utilizing a cloud-formed image.

Cloud computing hands off remote administrations including client information, programming, and handling.

Equipment and programming assets made open by means of the Web as controlled outsider administrations characterize cloud computing. Typically, these administrations give admittance to complex programming projects and premium organizations of server PCs.

Advanced Encryption Standard

The “Advanced Encryption Standard(AES)” may simply be the symmetric encryption strategy that is most utilized and celebrated today. Triple DES is actually one of the slower algorithms, and it comes a multiple time quicker than that.

Since the significant thing length of DES is far excessively little, an option become needed for it. It become thought about secure from top to bottom key request assault best with the development of computational ability. Triple DES become intended to manage this weakness, though flopping in its most extreme productive way, to be continuous witted.

The features of AES are as follows −

- “Symmetric key symmetric block cipher”
- “128-bit data, 128/192/256-bit keys”
- “Stronger and faster than Triple-DES”
- “Provide full specification and design details”
- “Software implementable in C and Java”

Operation of AES

Instead of a Feistel figure, AES is an iterative one. Its establishment is "replacement change organization". It comprises of a succession of connected tasks, some of which incorporate piece rearranging (changes) and others of subbing specific results for inputs.

Fascinatingly, AES utilizes bytes rather than bits for every one of the computations that it makes. AES thus in this way sees 128 pieces of a plaintext block as 16 bytes. For handling as a grid — these sixteen bytes are set in four lines and four sections.

Not in any regard like DES, the time of the significant thing decides the moved amount of rounds in AES in a separate way. Concerning encryption, for 128-digit keys AES utilizes 10 rounds, 192 piece keys utilizes 12 rounds and 256-bit keys utilizes 14 rounds. These those rounds takes an extra 128 - bit circular key from the essential AES key.

The accompanying picture shows the AES construction's schematic: -

Encryption Process

Here we just talk about the standard rounds of AES-S-Box. We can say that each round comprises of four sub-processes. The course of the fundamental round is as per the following:

“Byte Substitution (SubBytes)”

Investigating a fair table (S-box) decided in plan replaces the 16 information bits. The result turns out in a four-line by four-segment framework.

Shiftrows

All of the four framework columns is moved left. Each "tumble off" section is re-embedded on the right half of the column. Shift is finished as follows:

- The main column isn't changed.
- • One (byte) area in first line of second column is shifted left.
- Two maneuvers the third column two leftward.
- The fourth column is moved three leftward.
- • The result is another network with similar 16 bytes however moved concerning each other.

MixColumns

Four byte segments are currently different with a one of a kind numerical capability. If you input the four bytes of one section then it makes four entirely new bytes in elimination of the initial segment. This generates much one additional new grid with sixteen new bytes. It needs to be noted that the last round of the process does not include this stage.

Addroundkey

Presently seen as 128 pieces, the 16 grid bytes XOR the 128 pieces of the round key. Should this be the last round, the resultant ciphertext is In any case, we start another similar round and the resultant 128 pieces are viewed as 16 bytes.

Decryption Process

Decrypting of an AES ciphertext also uses similar characteristics as encryption with the only difference in the approach. Each cycle has the four methods did backward succession −

- “Add round key”
- “Mix columns”
- “Shift rows”
- “Byte substitution”

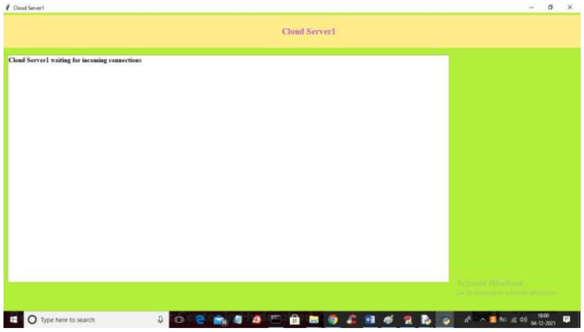
They assessment from a Feistel Code in that sub-approaches put in each circular disagreement opposite heading; even as they simultaneously join techniques, encryption/and unscrambling one ought to be utilized individually from the other.

AES Analysis

AES is frequently used and endorsed in both equipment and programming in academian and industrial cryptography in the present era. Not yet known are any helpful cryptanalytic assaults against AES. Besides, AES offers worked in key length adaptability that lets one fairly "future-confirmation" against progression in the limit with regards to careful key hunts.

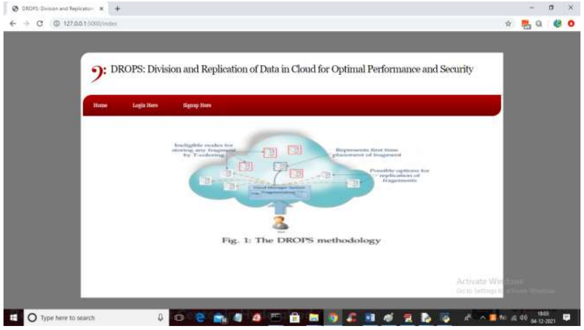
Nevertheless, as in the example of DES, the AES security is just possible if a competent key management is applied and if execution is well done.

5. EXPERIMENTAL RESULTS



Cloud Server1 waiting for incoming connections

“Fig.3: Cloud server1”

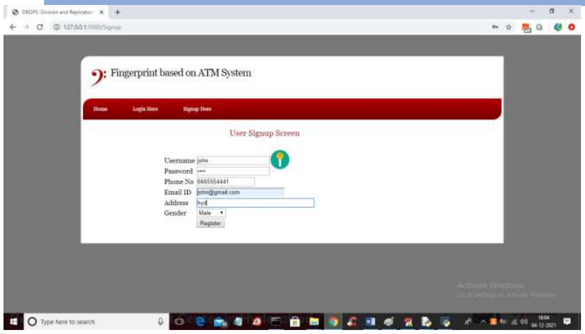


DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

Fig. 1: The DROPS methodology

DROPS: Division and Replication
127.0.0.1:5000/index
Home
Login Here
Signup Here
Ineligible nodes for storing any fragment by T-coloring
Represents first time placement of fragment
Possible options for replication of fragments
Activate Windows
Type here to search
18:03
04-12-2021

“Fig.4: Webpage”

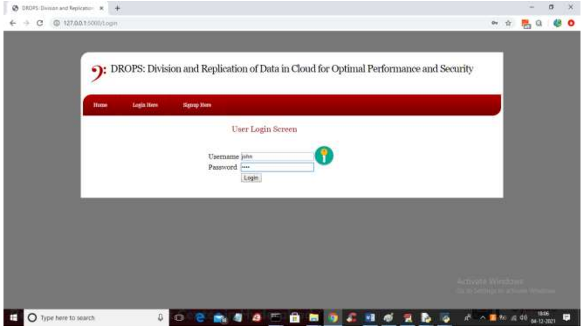


Fingerprint based on ATM System

User Signup Screen

Username john
Password ****
Phone No 6665554441
Email ID john@gmail.com
Address hyd
Gender Male

“Fig.5: User signup”

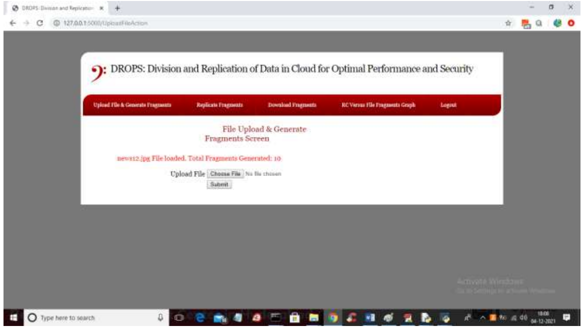


DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

User Login Screen

Username john
Password ****

“Fig.6: User login”



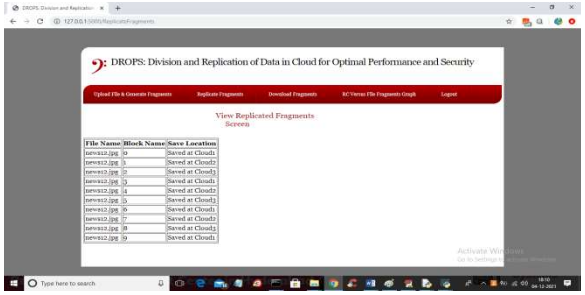
DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

File Upload & Generate Fragments Screen

news12.jpg File loaded. Total Fragments Generated: 10

Upload File No file chosen

“Fig.7: Upload file & generate fragments”

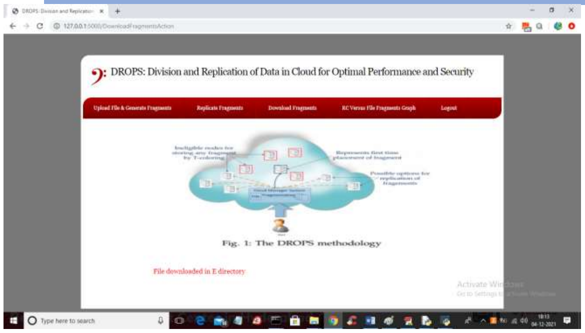

127.0.0.1:5000/ReplicateFragments
Upload File & Generate Fragments
Replicate Fragments
Download Fragments
RC Versus File Fragments Graph
Logout
Type here to search
Activate Windows

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

View Replicated Fragments Screen

File Name	Block Name	Save Location
news12.jpg	0	Saved at Cloud1
news12.jpg	1	Saved at Cloud2
news12.jpg	2	Saved at Cloud3
news12.jpg	3	Saved at Cloud1
news12.jpg	4	Saved at Cloud2
news12.jpg	5	Saved at Cloud3
news12.jpg	6	Saved at Cloud1
news12.jpg	7	Saved at Cloud2
news12.jpg	8	Saved at Cloud3
news12.jpg	9	Saved at Cloud1

“Fig.8: Replicate fragments”

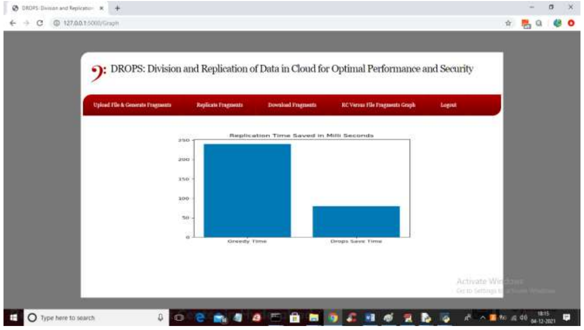


DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

127.0.0.1:5000/DownloadFragmentsAction
Upload File & Generate Fragments
Replicate Fragments
Download Fragments
RC Versus File Fragments Graph
Logout
Ineligible nodes for storing any fragment by T-coloring
Represents first time placement of fragment
Possible options for replication of fragments
Fig. 1: The DROPS methodology
Activate Windows
Type here to search
18:13
04-12-2021

File downloaded in E directory

“Fig.9: Download fragments”



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

“Fig.10: RC Versus File Fragments Graph”

6. CONCLUSION

In this paper we introduced the DROPS approach a safety framework of cloud storage inclined towards tending with the recovery time security and general execution. The information document was broken, and the pieces spread among a few hubs. T-shading let the hubs be isolated. The fracture and that's what conveyance ensured, should an assault find true success, no significant data could be tracked down by an adversary. Not one cloud hub, kept more than one part of a similar record. Dangers to inner legitimacy were contrasted and viewpoints which were possibly featured while explaining full scale replication procedures for the general show of the DROPS approach. The disclosures made by the proliferations communicated that the simultaneous thought on security and execution, delivered higher security level of data alongside somewhat little decrease in execution. Again currently utilizing the DROPS approach, a client downloads the record, change the things and subsequently transfer it. The upgrade of a modified update mechanism that can recognize and refresh just the basic region is, hence, vital. Yet again the recently referenced future undertakings will set aside the time and cash put resources into download, invigorate, and move the substance. Moreover, possible impacts of TCP in the cast toward DROPS ought to be talked about regarding dispersed data capacities and openness.

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 datacenter architectures,” Concurrency and Computation: Practice andExperience, 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 robustnessof 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 cloudcomputing systems,” In Proceedings of IEEE ComputerSociety Symposium on Research in Security and Privacy, OaklandCA, pp. 110-121, 1991.

[5] B. Grobauer, T.Walloschek, and E. Stocker, “Understandingcloud 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 computingstandards roadmap,” NIST Special Publication, July 2011.

[9] W. A. Jansen, “Cloud hooks: Security and privacy issues incloud computing,” In 44th Hawaii IEEE International ConferenceonSystem Sciences (HICSS), 2011, pp. 1-10.

[10] A. Juels and A. Opera, “New approaches to security andavailability 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.

[12] L. M. Kaufman, “Data security in the world of cloud computing,”IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

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

[14] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani,“Towards Secure Mobile Cloud Computing: A Survey,” FutureGeneration Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.

[15] A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, “Enhanceddynamic credential generation scheme for protectionof user identity in mobile-cloud computing, The Journal ofSupercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706 .

[16] Tejas Sanjeev Panse, Suket Gakhar, Anant Kumar, Lakshmi Narasimhan, “Systems and methods for cluster resource balancing in a hyper-converged infrastructure”, Available at: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=nkU6f3wAAAAJ&citation_for_view=nkU6f3wAAAAJ:u-x6o8ySG0sC

[17] Tejas Sanjeev Panse, Suket Gakhar, Anant Kumar, Lakshmi Narasimhan, “Fault tolerant hyper-converged infrastructure upgrades in an environment with no additional physical infrastructure”, Available at: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=nkU6f3wAAAAJ&citation_for_view=nkU6f3wAAAAJ:u5HHmVD_uO8C

[18] Tejas Sanjeev Panse, Suket Gakhar, Anant Kumar, Lakshmi Narasimhan, “Nested host manager in a hyper-converged infrastructure”, Available at: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=nkU6f3wAAAAJ&citation_for_view=nkU6f3wAAAAJ:WF5omc3nYNoC