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

Partition and Repetition of Data in Cloud for Finest Performance and Security

Shivangi R[1], Dr. Shiva Murthy G[2], Ramakrishna Prasad A. L.[3]

[1]M.Tech Student, Department of CSE, VTU CPGS, Muddenahalli, Chikkaballapura, India

[2]Head of Department, Department of CSE, VTU CPGS, Muddenahalli, Chikkaballapura, India

[3]Assistant Professor, Department of CSE, VTU CPGS, Muddenahalli, Chikkaballapura, India

Abstract: ***Outsourcing information to an outsider managerial control, as is done in distributed computing, offers ascend to security concerns. The information trade off may happen because of assaults by different clients and hubs inside the cloud. In this way, high safety efforts are required to ensure information inside the cloud. Be that as it may, the utilized security methodology should likewise consider the enhancement of the information recovery time. In this paper, we propose Partition and Repetition of Data in Cloud for Finest Performance and Security (PROPS) that on the whole methodologies the security and execution issues. In the PROPS system, we partition a record into sections, and recreate the divided information over the cloud hubs. Each of the hubs stores just a solitary piece of a specific information document that guarantees that even in the event of an effective assault, no important data is uncovered to the aggressor. Additionally, the hubs putting away the pieces are isolated with certain separation by methods for chart T-shading to preclude an aggressor of speculating the areas of the sections. Besides, the PROPS approach does not depend on the conventional cryptographic strategies for the information security; accordingly diminishing the arrangement of computationally costly techniques. We demonstrate that the likelihood to find and trade off the greater part of the hubs putting away the pieces of a solitary document is to a great degree low. We additionally look at the execution of the PROPS approach with ten different plans. The more elevated amount of security with slight execution overhead was watched.***

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

1. Introduction

The distributed computing worldview has improved the utilization and administration of the data innovation foundation. Distributed computing is described by on-request self-administrations; universal system gets to, asset pooling, flexibility, and measured administrations. The previously mentioned qualities of distributed computing make it a striking hopeful for organizations, associations, and individual clients for selection. Notwithstanding, the advantages of ease, irrelevant administration (from a clients viewpoint), what's more, more noteworthy adaptability accompanied expanded security concerns. Security is a standout amongst the most pivotal angles among those precluding the across the board appropriation of cloud processing. Cloud security issues may stem.

Because of the center technology's execution (virtual machine (VM) escape, session riding, and so forth.), cloud benefit offerings (organized inquiry dialect infusion, frail verification plans, and so on.), and emerging from cloud attributes (information recuperation helplessness, Internet convention weakness, and so on.). For a cloud to be secure, the greater part of the taking part elements must be secured. In any given framework with different units, the most elevated level of the systems security is equivalent to the security level of the weakest substance. Along these lines, in a cloud, the security of the benefits does not exclusively rely on upon a person's safety efforts. The neighboring substances may give a chance to an aggressor to sidestep the client's barriers. The off-site information stockpiling cloud utility requires clients to move information in cloud's virtualized and shared condition that may bring about different security concerns. Pooling and flexibility of a cloud, permits the physical assets to be shared among numerous clients. Besides, the common assets might be reassigned to different clients at some example of time that may come about in information bargain through information recuperation systems. Moreover, a multi-inhabitant virtualized condition may bring about a VM to get away from the limits of virtual machine screen (VMM). The got away VM can meddle with different VMs to approach unapproved information. Thus, cross-occupant virtualized organize get to may likewise bargain information protection also, honesty. Uncalled for media sterilization can likewise spill customers private information.

The information outsourced to an open cloud must be secured. Unapproved information access by different clients and forms (regardless of whether incidental or think) must be avoided. As talked about over, any feeble substance can put the entire cloud at hazard. In such a situation, the security component should generously increment an aggressor's push to recover a sensible sum of information even after a fruitful interruption in the cloud. Additionally, the likely measure of misfortune (because of information spillage) should likewise be limited. A cloud must guarantee throughput, unwavering quality, and security. A key element deciding the throughput of a cloud that stores information is the information recovery time. In expansive scale frameworks, the issues of information unwavering quality, information accessibility, and reaction time are managed with information replication methodologies. Be that as it may, setting imitations information over various hubs builds the assault surface for that specific information. For example, putting away m reproductions of a record in a cloud rather than one reproduction builds the likelihood of a hub holding document to be picked as assault casualty, from 1 n to m n , where n is the aggregate number of hubs. From the above exchange, we can find that both security and execution are basic for the cutting edge expansive scale

frameworks, for example, mists. Along these lines, in this paper, we on the whole approach the issue of security and execution as a protected information replication issue. We introduce Partition and Repetition of Data in the Cloud for Optimal Performance also; Security (PROPS) that judicially pieces client documents into pieces and recreates them at key areas inside the cloud. The division of a document into sections is performed in view of a given client criteria to such an extent that the individual pieces don't contain any important data.

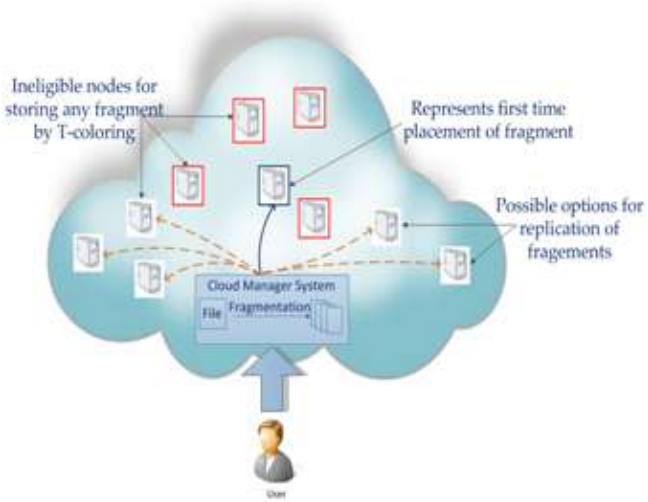

Figure 1: PROPS Methodology

2. Our Contributions

In this paper, we propose a novel two-factor security instrument for information put away in the cloud. Our component gives the accompanying pleasant elements:

1) Our framework is an IBE (Identity-based encryption) based instrument. That is, the sender just needs to know the character of the recipient keeping in mind the end goal to send an encoded information (cipher text) to him/her. No other data of the collector (e.g. open key, authentication and so on.) is required. At that point the sender sends the cipher text to the cloud where the collector can download it at whenever.
2) Our framework gives two-figure information encryption security. Keeping in mind the end goal to decode the information put away in the cloud, the client needs to have two things. In the first place, the client needs his/her mystery key which is put away in the PC. Second, the client needs to have a one of a kind individual security gadget which will be utilized to interface with the PC (e.g. USB, Bluetooth and NFC). It is difficult to unscramble the cipher text without either piece.
3) More critically, our framework, interestingly, gives security gadget (one of the components) revocability. Once the security gadget is stolen or detailed as lost, this gadget is disavowed. That is, utilizing this gadget can no longer decode any cipher text (comparing to the client) in any situation. The cloud will instantly execute a few calculations to change the current cipher text to be un-decrypt able by this gadget. While the client needs to utilize his new/substitution gadget (together with his mystery key) to unscramble his/her cipher text. This procedure is totally straightforward to the sender.
4) The cloud server can't unscramble any ciphertext at whatever time. We give an estimation of the running time of our model to demonstrate its common sense, utilizing some benchmark comes about. We likewise take note of that in spite of the fact that there exist a few innocent methodologies that appear to accomplish our objective,

3. Model Overview

We first give an instinct on it. In our framework, we have the accompanying elements:

- We build up a plan for outsourced information that considers both the security and execution. The proposed plot sections and duplicates the information record over cloud hubs.
- The proposed PROPS plot guarantees that even on account of an effective assault, no significant data is uncovered to the assailant.
- We don't depend on customary cryptographic strategies for information security. The non-cryptographic nature of the proposed plot makes it quicker to play out the required operations (position and recovery) on the information.

We guarantee a controlled replication of the record pieces, where each of the parts is recreated once with the end goal of enhanced security.

We additionally delineate our instrument's structure in Fig. At the point when another framework client, say Bob, joins our framework, a PKG will issue a private key, and SDI will issue a security gadget to him. Both the private key and the security gadget are important for recuperating information from its encoded arrange. In normal information sharing, an information sender, say Alice, first scrambles the sharing information under the personality of an information beneficiary, say Bob, and next transfers the cipher text to the cloud server. Here we allude to this cipher text as first level cipher text. In the wake of accepting the main level cipher text from Ali, the cloud server then turns the cipher text to turn into a moment level cipher text for the relating security gadget having a place with Bob. Weave then downloads the second-level cipher text from the cloud, and next recoups the information from its scrambled shape by utilizing his private key and security gadget.

At the point when the security gadget of Bob is either lost or stolen, Weave first reports the issue to the SDI. The SDI then issues another security gadget to Bob, and in the interim, it sends a demand of refreshing Bob's comparing cipher text alongside a unique key to the cloud server. The cloud server refreshes the cipher texts of Bob under an old security gadget to the ones under another gadget. In any case, it doesn't access the fundamental information in the refresh procedure. Here Bob is permitted to download furthermore, recoup the information by utilizing his private key and new security gadget.

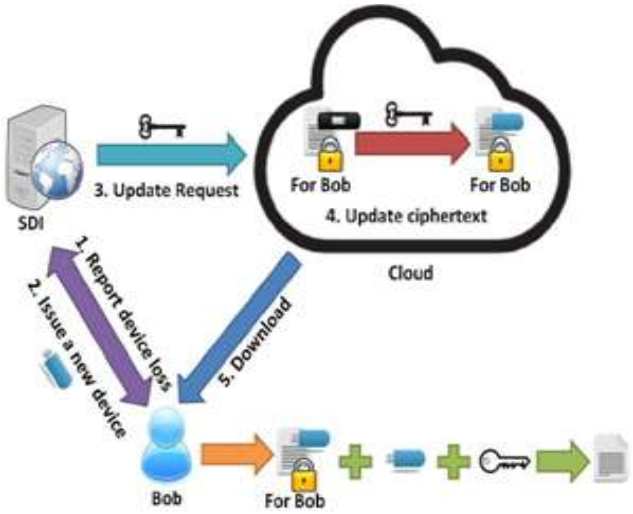

Figure 2: Development Road Map

Our Setup

Development Road map. We use two diverse encryption innovations: one is IBE and the other is conventional Open Key Encryption (PKE). We first permit a client to create a first level cipher text under a recipient's character. The primary level cipher text will be further changed into a moment level cipher text comparing to a security gadget. The subsequent cipher text can be unscrambled by a legitimate beneficiary with mystery key and security gadget. Here, one may question that our development is an inconsequential and clear mix of two unique encryptions.

Cipher text and the refreshed cipher text. We facilitate utilize hash-signature technique to "sign" cipher text such that once a segment of cipher text is tempered by foe, the cloud and cipher text recipient can tell. From the above introductions, we can see that our two factor insurance framework with security gadget revocability can't be gotten by insignificantly joining an IBE with a PKE.

Algorithm 1 Algorithm for fragment placement

Intputs and intializations:

$O = \{ O_1, O_2, \ldots, O_N\}$
$o = \{\text{sizeof}(O_1), \text{sizeof}(O_2), \ldots, \text{sizeof}(O_N)\}$
col = { open_color, close_color }
$cen = \{cen_1, cen_2, \ldots, cen_M\}$
$col \leftarrow$ open_color $\forall$ i
$cen \leftarrow cen_i \forall i$
Compute:
for each $O_k \in O$ do
select $S^i \mid S^i \leftarrow$ indexof (max(cen_i)
if col_S^i = open_color and $s_i >= o_k$ then
$S^i \leftarrow O_k$
$s_i \leftarrow s_i - o_k$
$col_S^i \leftarrow$ close_color
$S^{i'} \leftarrow$ distance (S^i, T) /* returns all nodes at T from S^i and stores in temporary set $S^{i'}$ * /
$col_S^{i'} \leftarrow$ close_color
end if
end for

4. Experimental Results

We compared the performance of the PROPS methodology with the algorithms. The behavior of the algorithms was studied by:

- Increasing the number of nodes in the system.
- Increasing the number of objects keeping number of nodes constant.
- Changing the nodes storage capacity, and
- Varying the read/write ratio. The aforesaid parameters are significant as they affect the problem size and the performance.

Performance Graph:

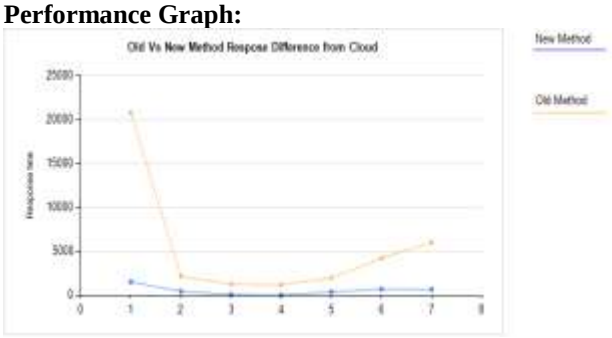

Figure 3: Old vs New method

Result data

Table 1: Performance measure of Old vs New method

SL No	Drops Performance		PROPS Performance	
1	1.5KB	22000msec	1KB	250msec
2	2KB	2500 msec	2KB	100msec
3	3KB	1000msec	3KB	50msec
4	4KB	500msec	4KB	20msec

5. Conclusion

We proposed the PROPS philosophy, a distributed storage security conspire that by and large manages the security and execution as far as recovery time. The information record was divided and the pieces are scattered over numerous hubs. The hubs were isolated by methods for T-shading. The fracture and dispersal guaranteed that no huge data was reachable by a foe if there should arise an occurrence of an effective assault. No hub in the cloud, put away more than a solitary part of a similar record. The execution of the PROPS procedure was contrasted and full-scale replication systems. The aftereffects of the reproductions uncovered that the synchronous concentrate on the security furthermore, execution, brought about expanded security level of information joined by a slight execution drop. Right now with the PROPS approach, a client has to download the record, refresh the substance, and transfer it once more. It is vital to build up a programmed refresh system that can distinguish and refresh the required sections as it were. The previously mentioned future work will spare the time and assets used in downloading, refreshing, furthermore, transferring the record once more. Besides, the ramifications of TCP in cast over the PROPS procedure should be examined that is significant to circulated information stockpiling and get to.

6. Acknowledgement

I would like to express my special thanks of gratitude to Assistant professor. Mr. Ramakrishna Prasad A.L, Department of Computer Science and Engineering, Visvesvaraya Institute of Advanced Technology. who gave me the golden opportunity to do this wonderful project on the topic (An Optimized task Scheduling Algorithm and Maintaining Load in Cloud Computing), which also helped me in doing a lot of research and I came to know about so many new things I are really thankful to him. And, secondly I would also like to thank my parents who helped me a lot in finalizing this project within the limited time frame.

References

[1] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani,. 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 distributedcomputing 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 in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.

[10] 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.

[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 Distributed Computing, Vol. 68, No. 2, 2008,pp. 113-136.

[14] 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] 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] T. Loukopoulos and I. Ahmad, "Static and adaptive distributeddata replication using genetic algorithms," Journal ofParallel and Distributed Computing, Vol. 64, No. 11, 2004, pp.1270-1285.

[17] Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragmentand replica allocation in large-scale distributed file systems,"IEEE Transactions on Parallel and Distributed Systems, Vol.14, No. 9, 2003, pp. 885-896.

[18] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, "On theplacement of web server replicas," In Proceedings of INFOCOM2001, Twentieth Annual Joint Conference of the IEEE Computer andCommunications Societies, Vol. 3, pp. 1587-1596, 2001.

[19] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying andanalyzing security, privacy and trust issues in cloud computing environments," Procedia Engineering, Vol. 15, 2011, pp. 28522856.

[20] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure overlaycloud storage with access control and assured deletion," IEEETransactions on Dependable and Secure Computing, Vol. 9, No. 6,Nov. 2012, pp. 903-916.

[21] M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, "On theoptimal placement of secure data objects over Internet," InProceedings of 19th IEEE International Parallel and DistributedProcessing Symposium, pp. 14-14, 2005.

[22] D. Zissis and D. Lekkas, "Addressing cloud computing securityissues," Future Generation Computer Systems, Vol. 28, No. 3,2012, pp. 583-592.

[23] 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 survivablestorage system," Carnegie Mellon University, Technical ReportCMU-CS-01-120, May 2001.

[24] M. Newman, Networks: An introduction, Oxford UniversityPress, 2009.

[25] R. Khan, M. Othman, S. A. Madani, S. U. Khan,"A survey of mobile cloud computing applicationmodels," IEEE Communications Surveys and Tutorials, DOI:10.1109/SURV.2013.062613.00160.