ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

A Review on Data Fragmentation and Replica Allocation with Optimal Performance and Security in Cloud Mechanism

Nishant Kumar[1], Amol Ganorkar[2], Girish Kakade[3], Mayur Ekal[4], Rohit Bamane[5]

Student, Dept. of CS, Pad.Dr.D Y Patil College of Engineering and Technology, Pimpri, Savitribai Phule Pune University, Pune, India[1,2,3,4]

Professor, Dept. of CS, Pad.Dr.D Y Patil College of Engineering and Technology, Pimpri, Savitribai Phule Pune University, Pune, India[5]

ABSTRACT: These days, more ventures and associations are facilitating their information into the cloud, so as to lessen the IT support cost and upgrade the information dependability. The general existing conditions is that clients as a rule put their information into a solitary cloud (which is liable to the seller lock-in danger) and after that just trust to luckiness. Outsourcing information to an outsider managerial control, as is done in distributed computing, offers ascend to security concerns. The information trade off might happen because of assaults by different clients and hubs inside of the cloud. Subsequently, high efforts to establish safety are required to ensure information inside of the cloud. Nonetheless, the utilized security technique should likewise consider the improvement of the information recovery time. In this approach, we separate a document into sections, and reproduce the divided information over the cloud hubs. Each of the hubs stores just a solitary piece of a specific information record that guarantees that even if there should be an occurrence of an effective assault, no important data is uncovered to the assailant. In addition, the hubs putting away the parts are isolated with certain separation by method for diagram T-shading to restrict an assailant of speculating the areas of the pieces. We additionally propose an open evaluating plan for the recovering code-based distributed storage. To take care of the recovery issue of fizzled authenticators without information proprietors, we present an intermediary, which is advantaged to recover the authenticators, into the conventional open inspecting framework model. Consequently, our plan can totally discharge information proprietors from online weight.

KEYWORDS: Cloud storage,Cloud Security,Fragmentation, Replication, Performance, Public Audit.

I. INTRODUCTION

Distributed storage is currently picking up fame since it offers an adaptable on-interest information outsourcing administration with engaging advantages: alleviation of the weight for capacity administration, all inclusive information access with area freedom, and evasion of capital use on equipment, programming, and individual systems of support, and so forth. By the by, this new worldview of information facilitating benefit additionally brings new security dangers toward client's information, subsequently making people or enterprisers still feel reluctant. It is noticed that information proprietors lose extreme control over the destiny of their outsourced information; along these lines, the accuracy, accessibility and honesty of the information are being put at danger. From one perspective, the cloud administration is normally confronted with an expansive scope of inside/outside enemies, who might malignantly erase or degenerate clients' information; then again, the cloud administration suppliers might act deceptively, endeavoring to shroud information misfortune or debasement and asserting that the records are still accurately put away in the cloud for notoriety or money related reasons. In this manner it bodes well for clients to execute an effective convention to perform periodical confirmations of their outsourced information to guarantee that the cloud for sure keeps up their information accurately.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

Security is a standout amongst the most pivotal angles among those denying the far reaching reception of distributed computing. Cloud security issues might stem because of the center innovation's usage (virtual machine (VM) escape, session riding, and so on.), cloud administration offerings (organized inquiry dialect infusion, feeble confirmation plans, and so on.), and emerging from cloud qualities (information recuperation weakness, Internet convention helplessness, and so forth) for a cloud to be secure, the majority of the taking part elements must be secure. In any given framework with different units, the most elevated amount of the framework's security is equivalent to the security level of the weakest element. In this manner, in a cloud, the security of the benefits does not exclusively rely on upon an individual's efforts to establish safety. The neighboring elements might give a chance to an aggressor to sidestep the client's resistances.

The off-site information stockpiling cloud utility obliges clients to move information in cloud's virtualized and shared environment that might bring about different security concerns. Pooling and versatility of a cloud, permits the physical assets to be shared among numerous clients. In addition, the mutual assets might be reassigned to different clients at some occasion of time that might bring about information bargain through information recuperation procedures. Besides, a multi-inhabitant virtualized environment might 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 have entry to unapproved information. Likewise, cross-occupant virtualized system access might likewise bargain information security and trustworthiness. Uncalled for media sterilization can likewise release client's private information.

II. RELATED WORK

1) Paper Name: -On the characterization of the structural robustness of data center networks.

Authors: -K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

Abstract: -Data centers being an architectural and functional block of cloud computing are integral to the Information and Communication Technology (ICT) sector. Cloud computing is rigorously utilized by various domains, such as agriculture, nuclear science, smart grids, healthcare, and search engines for research, data storage, and analysis. A Data Center Network (DCN) constitutes the communicational backbone of a data center, ascertaining the performance boundaries for cloud infrastructure. The DCN needs to be robust to failures and uncertainties to deliver the required Quality of Service (QoS) level and satisfy Service Level Agreement (SLA). In this paper, we analyze robustness of the state-of-the-art DCNs. Our major contributions are: (a) we present multi-layered graph modeling of various DCNs; (b) we study the classical robustness metrics considering various failure scenarios to perform a comparative analysis; (c) we present the inadequacy of the classical network robustness metrics to appropriately evaluate the DCN robustness; and (d) we propose new procedures to quantify the DCN robustness. Currently, there is no detailed study available centering the DCN robustness. Therefore, we believe that this study will lay a firm foundation for the future DCN robustness research.

2) Project Name: -Intrusion tolerance in distributed computing systems.

Authors: -Y. Deswarte, L. Blain, and J-C. Fabre, In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.

Abstract: -An intrusion-tolerant distributed system is a system which is designed so that any intrusion into a part of the system will not endanger confidentiality, integrity and availability. This approach is suitable for distributed systems, because distribution enables isolation of elements so that an intrusion gives physical access to only a part of the system. In particular, the intrusion-tolerant authentication and authorization servers enable a consistent security policy to be implemented on a set of heterogeneous, untrusted sites, administered by untrusted (but non conspiring) people. The authors describe how some functions of distributed systems can be designed to tolerate intrusions. A prototype of the persistent file server presented has been successfully developed and implemented as part of the Delta-4 project of the European ESPRIT program.

3) Project Name: -Understanding cloud computing vulnerabilities

Authors: - B. Grobauer, T.Walloschek, and E. Stocker, IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

Abstract: -The current discourse about cloud computing security issues makes a well-founded assessment of cloud computing's security impact difficult for two primary reasons. First, as is true for many discussions about risk, basic vocabulary such as "risk," "threat," and "vulnerability" are often used as if they were interchangeable, without regard to their respective definitions. Second, not every issue that's raised is really specific to cloud computing. We can achieve an accurate understanding of the security issue "delta" that cloud computing really adds by analyzing how cloud computing influences each risk factor. One important factor concerns vulnerabilities: cloud computing makes certain well-understood vulnerabilities more significant and adds new vulnerabilities. Here, the authors define four indicators of cloud-specific vulnerabilities, introduce a security-specific cloud reference architecture, and provide examples of cloud-specific vulnerabilities for each architectural component.

4) Project Name:-Secure dynamic fragment and replica allocation in large-scale distributed file system

Authors:- A. Mei, L. V. Mancini, and S. Jajodia, " IEEE Transactions on Parallel and Distributed Systems, Vol.14, No. 9, 2003, pp. 885-896.

Abstract: - We present a distributed algorithm for file allocation that guarantees high assurance, availability, and scalability in a large distributed file system. The algorithm can use replication and fragmentation schemes to allocate the files over multiple servers. The file confidentiality and integrity are preserved, even in the presence of a successful attack that compromises a subset of the file servers. The algorithm is adaptive in the sense that it changes the file allocation as the read-write patterns and the location of the clients in the network change. We formally prove that, assuming read-write patterns are stable, the algorithm converges toward an optimal file allocation, where optimality is defined as maximizing the file assurance.

5) Project name-Surveying and analyzing security, privacy and trust issues in cloud computing environments

Authors- D. Sun, G. Chang, L. Sun, and X. Wang, "Procedia Engineering, Vol. 15, 2011, pp. 2852 2856

Abstract: -

Cloud computing is almost similar distributed computing over a network and means the power to run a program on many connected computers at the same time. The word is also, more commonly used to refer to network-based services which seems to be provided by real server hardware, which really are served up by virtual hardware, simulated by software running on one or more real machines. Such type of virtual servers do not physically exist and can therefore be moved around and scaled up or scale down on the fly without affecting the end user - arguably, rather like a cloud. Cloud computing is a model to achieve more reliable, on-demand access to a shared pool configurable computing resources. In cloud computing, IT related abilities are provided as services, accessible without requiring brief information of the underlying technologies, and with minimal management effort. It provides more efficient computing by centralizing storage, bandwidth and memory processing. Adopting cloud computing can result in both negative and positive effects on data security. This paper provides an overview of cloud computing, and discusses related security challenges. We emphasize that even there are many techniques that can improve cloud security, there are in present no one-size fits-all solutions, and future work has to undertake challenges such as service level agreements for security, as well as holistic schemes for insure accountability in the cloud.

III. CONTRIBUTION

As a contributive part we are actualizing open evaluating which keeps up information respectability. To completely guarantee the information uprightness and recovery the clients' calculation assets and also online weight, we propose an open reviewing plan for the recovering code-based distributed storage, in which the honesty checking and recovery (of fizzled information pieces and authenticators) are actualized by an outsider evaluator and a semi-trusted intermediary independently for the information proprietor. Additionally, we "scramble" the coefficients to secure information protection against the evaluator, which is more lightweight than applying the confirmation blind procedure.

IV. PROPOSED METHODOLOGY AND DISCUSSION

When data owner wants to send file on cloud server first file is dividing into fragments and then fragments are encrypted. These encrypted fragments are then send to cloud server. These fragments are then allocated using concept

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

of T-coloring graph on cloud server. To maintain integrity we are using the Third Party Auditor (TPA) which makes the audit of the stored file on cloud and sent audit report to the data owner by mail. If the file is modified by attacker then TPA sends audit report as modified file to data owner and Proxy Agent which replace the modified code with original contents.

V. ARCHITECTURE

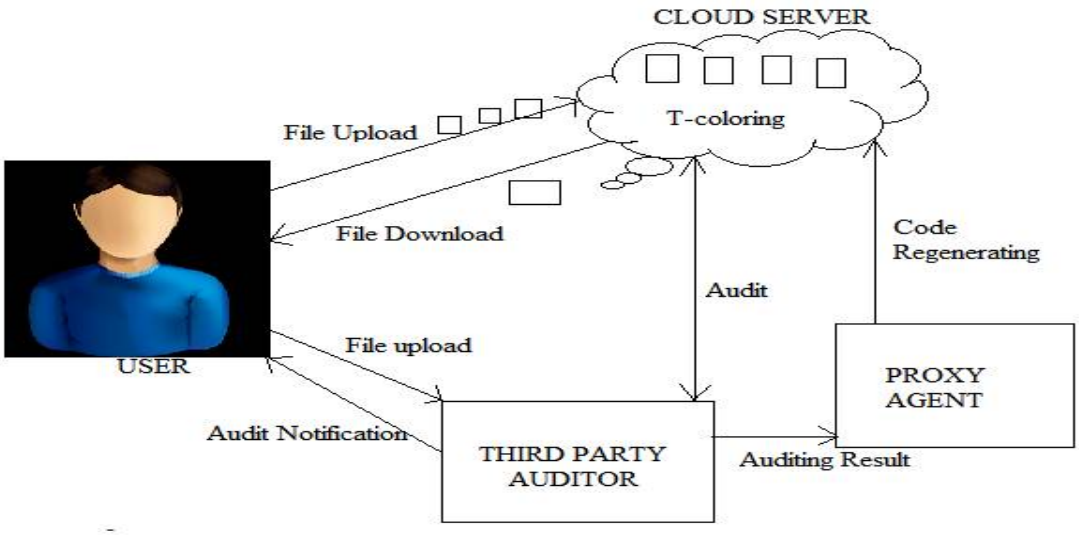

Fig No 01. DROPS Architecture

VI. CONCLUSION

We propose a methodology which deals with cloud storage security and optimal performance in terms of retrieval time. Before uploading file we are fragmenting that file into multiple fragments and allocate that fragments using T-coloring technique in cloud. This providessecurity at client level as well as in network layer. The fragmentation anddispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file.To protect the original data privacy against the TPA, we randomize the coefficients in the beginning ratherthan applying the blind technique during the auditing process. Considering that the data owner cannot always stay online in practice, in order to keep the storage available and verifiable after a malicious corruption, we introduce a semi-trusted proxy into the system model and provide a privilege for the proxy to handle the reparation of the coded blocks and authenticators.

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. Y. Deswarte, L. Blain, and J-C. Fabre "Intrusion tolerance in distributed computing systems." In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.
3. B. Grobauer, T.Walloschek, and E. Stocker "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
4. A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003, pp. 885-896.
5. D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," Procedia Engineering, Vol. 15, 2011, pp. 2852 2856