iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** VIII **Month of publication:** August 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.45151

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue VIII August 2022- Available at www.ijraset.com*

# Optimal Performance of Security by Fragmentation and Replication of Data in Cloud

Mrs. K. Rajani [1], Y. Sreeja[2], T. Tejaswini[3], B. Manasa[4]
[1, 2, 3]*Undergraduate Student,* [4]*Assistant Professor, Department of Computer Science Engineering Sridevi Women's Engineering College, Hyderabad*

***Abstract:*** ***Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval 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 replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker.***

## I. INTRODUCTION

### A. *Purpose*

The cloud computing paradigm has reformed the usage and management of the information technology infrastructure. Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The a forementioned characteristics of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. However, the benefits of low-cost, negligible management , and greater flexibility come with increased security concerns. Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technology's implementation, cloud service offerings, and arising from cloud characteristics.

### B. *Scope*

The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. As discussed above, any weak entity can put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase an attacker's effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud. 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 system′ s security is equal to the security level of the weakest entity. Therefore, in a cloud, the security of the assets does not solely depend on an individual's security measures. The neighboring entities may provide an opportunity to an attacker to bypass the users defenses Moreover, the probable amount of loss must also be minimized. The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.

### C. *Model Diagram/Overveiw*

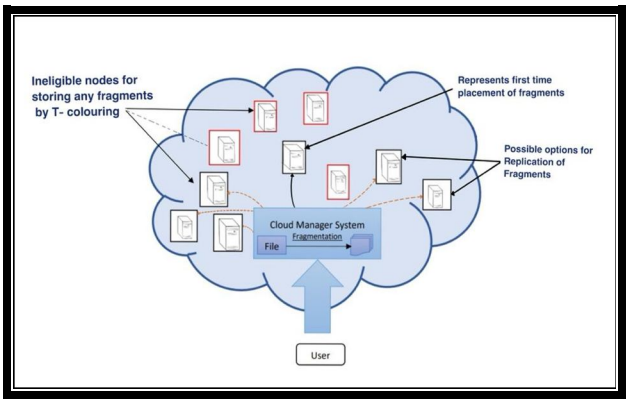



Fig. Model Diagram

The above model diagram depicts how the Cloud Manager System functions and how the files gets fragmented.

## II. SYSTEM ANALYSIS

### A. *Existing System*

Juels presented a technique to ensure the integrity, freshness, 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 freshness of the data using a Merkle tree. The file blocks, MAC codes, and version numbers are stored at various levels of the tree. G. Kappeset. al. approached the virtualized and multi-tenancy related issues in the cloud storage by utilizing the consolidated storage and native access control. The Dike authorization architecture is proposed that combines the native access control and the tenant name space isolation.

#### *1) Disadvantages Of Existing System*

The leakage of critical information in case of improper sanitization and malicious VM is not handled. Such schemes do not protect the data files against tempering and loss due to issues arising from virtualization and multi-tenancy. The data files are not fragmented and are handled as a single file.

### B. *Problem Statement*

The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval 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.

### C. *Proposed System*

Here, we collectively approach the issue of security and performance as a secure data replication problem. We present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially 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.We develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes.

#### *1) Advantages Of Proposed System*

The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.We do not rely 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 ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.

## III. SYSTEM REQUIREMENT

Specification

### A. *Functional Requirements*

*1)* Upload File
*2)* Generate Fragments
*3)* Replicate Fragments
*4)* Download File

### B. *Nonfunctional Requirements*

Non-functional requirement specifies the quality attribute of a software system. They judge the software system base on Security, Responsiveness, Usability,, Portability and other non-functional standards that are critical to the success of the software system.

*1)* Scalability
*2)* Interoperability
*3)* Reliability

*C. Hardware Requirements*

Minimum hardware requirements are very dependent on the particular software being developed by a given Enthought Python / Canopy / VS Code user. Applications that need to store large arrays/ objects in memory will require more RAM, whereas applications that need to perform numerous calculations or tasks more quickly will require a faster processor.

1) *Operating System:* windows,linux
2) *Processor:* minimum intel i3
3) *Ram:* minimum 4GB
4) *Hard Disk:* minimum 250gb

*D. Software Requirements*

The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints and user documentation. The appropriation of requirements and implementation constraints gives the general overview of the project in regards to what the areas of strength and deficit are and how to tackle them.

1) *Technology:* Python
2) *Web Server:* Flask

## IV. SYSTEM DESIGN

*A. System Architecture*

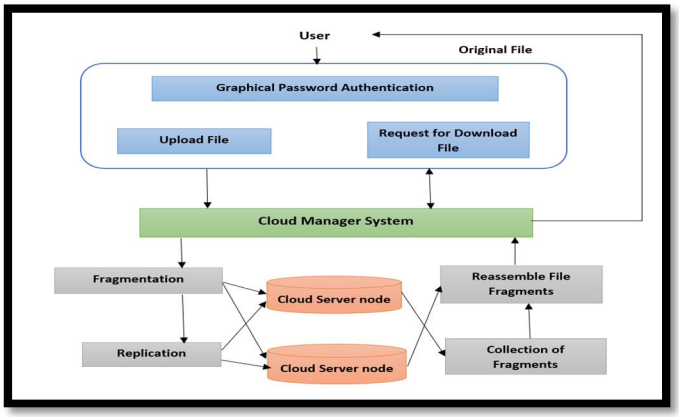



Fig SYSTEM ARCHITECTURE

The architecture diagram of the system shown below helps us to understand the system. In this composition, as a secure data replication problem we collectively approach the issue of certificate and performance. We present free fall that fragments user filing cabinet into art object and replicates them at strategic fix within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragment do not contain any meaningful information. Each of the cloud client(we use the term node to represent computing, reposition, physical, and virtual machines) contains a distinct fragment to increase the data security .

1) *Major Contributes:* We develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. We do not rely 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 ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.
2) System Components (Modules): In propose paper author is performing followings steps

a) *Module 1:* Upload File And Generate Fragments -we develop User and Cloud entities. In User entity, a user can upload a new File, Update uploaded File blocks.
b) *Module 2:* Replicate Fragments- Data replication is done by storing data copies at multiple clouds.
c) *Module 3:* Download Fragments- User can download the file when required.
d) *Module 4:* RC Versus File Fragments Graph- It can be observed from the plots that the increase in the number of file fragments reduced the performance of the algorithm.

## V. CONCLUSION

The following conclusions can be presented :

*1)* Firstly ,We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring.

*2)* Secondly, The fragmentation and dispersal 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. The performance of the DROPS methodology was compared with full-scale replication techniques.

*3)* Thirdly, The results of the simulations revealed that the simultaneous focus on the security and performance, resulted in increased security level of data accompanied by a slight performance drop. Currently with 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 aforesaid 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.

## VI. FUTURE ENHANCEMENT

Currently with 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 aforesaid 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.

## 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 and Experience, Vol. 25, No. 12, 2013, pp. 1999.

[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 distributed computing systems,” In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, OaklandCA, pp. 110-121, 2010.

[5] B. Grobauer, T.Walloschek, and E. Stocker, “Understanding cloud 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. 2013.

[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.

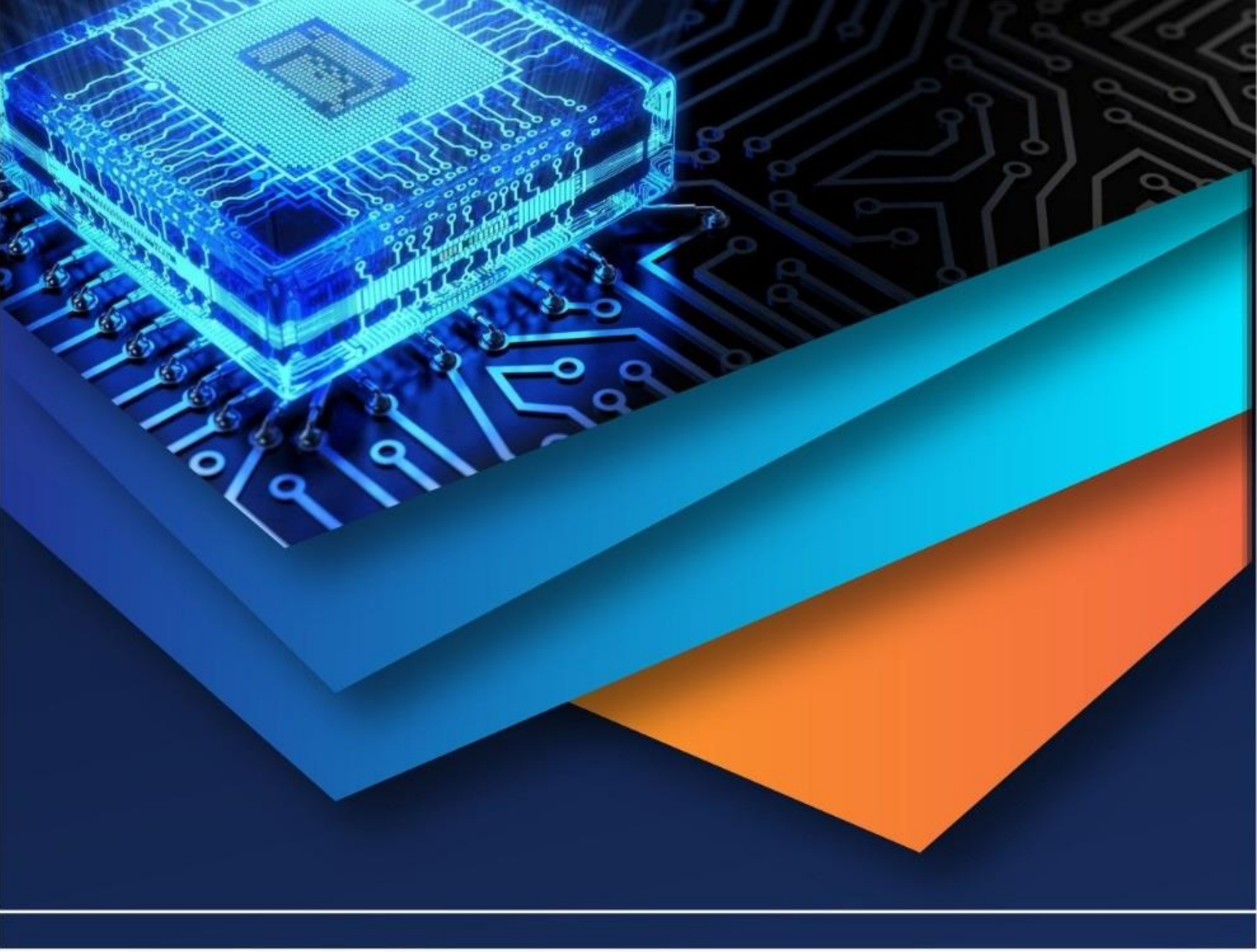
TEXTBOOKS:

1) Programming Python, Mark Lutz
2) Head First Python, Paul Barry
3) Core Python Programming ,R. Nageswara Rao
4) Learning with Python, Allen B. Downey

WEBSITES

1) https://www.w3schools.com/python/
2) https://www.tutorialspoint.com/python/index.htm
3) https://www.javatpoint.com/python-tutorial
4) https://www.learnpython.org/
5) https://www.pythontutorial.net/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY