IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |

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

Mr. Rameswara Annad, K. Umesh, M. Akhil, S. Rohith Kumar

Assistant Professor, Department of Computer Science and Engineering, Anurag Group of Institutions, Hyderabad, India

Students, Department of Computer Science and Engineering, Anurag University, Hyderabad, India

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 withinthe cloud. However, the employed security strategy must also take into account the optimization ofthe 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. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore,the DROPS methodology does not rely on the traditional cryptographic techniques for the datasecurity; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file isextremely low. We also compare the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

KEYWORDS: Centrality, cloud security, fragmentation, replication, performance.

I. INTRODUCTION

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 aforementioned 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 (from a users perspective), 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 (virtual machine (VM) escape, session riding, etc.), cloud service offerings (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.). For a cloud to be secure, all of the participating entities must besecure. 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. The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physical resources to be shared among many users. Moreover, the shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies. Furthermore, a multi-tenant virtualized environment may result in a VM to escape the bounds of virtual machine monitor (VMM). The escaped VM can interfere with other VMs to have access to unauthorized data. Similarly, cross-tenant virtualized network access may also compromise data privacy and integrity. Improper media sanitization can also leak customer′ s private data. The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes (whether accidental or deliberate) 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. Moreover, the probable amount of loss (as a result of data leakage) must also be minimized.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |

II. RELATED WORK

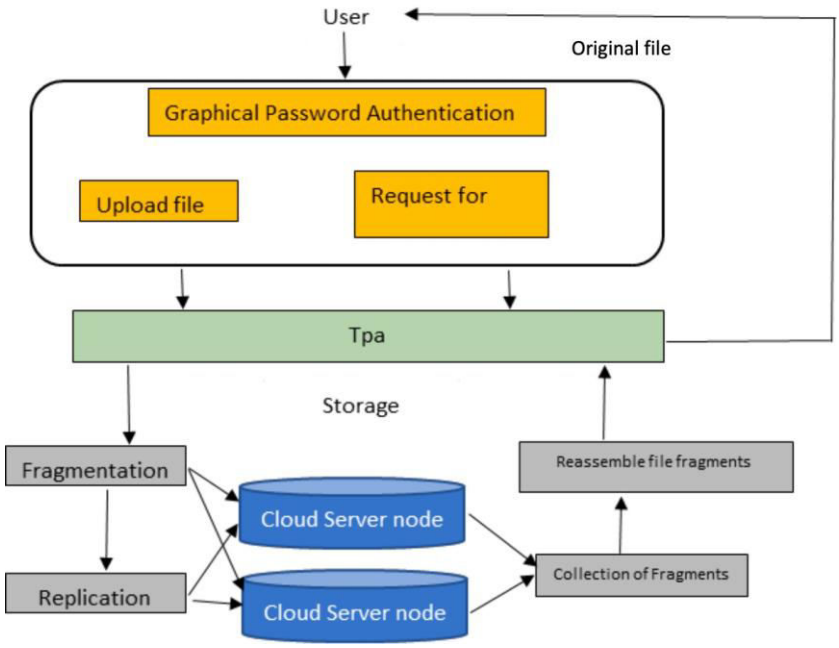
- The Juels et al. presented a technique to ensure the integrity, freshness, and availability of data in a cloud.
- The data migration to the cloud is performed by the Iris file system. A gateway application is designed an employed in the organization that ensures the integrity and freshness of the data using a Merkle tree. The file blocks, MAC codes, and version numbers are stored at various levels of the tree.
- G. Kappes et. 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.

III. EXISTING METHOD

- Due to concerns originating from virtualization and multi-tenancy, such techniques do not safeguard the data files against tampering and loss.
- The data files are processed as a single file and are not fragmented.

IV. PROPOSED METHOD

In this paper, we collectively approach the issue of security and performance as a secure datareplication 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 replicatesthem 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.



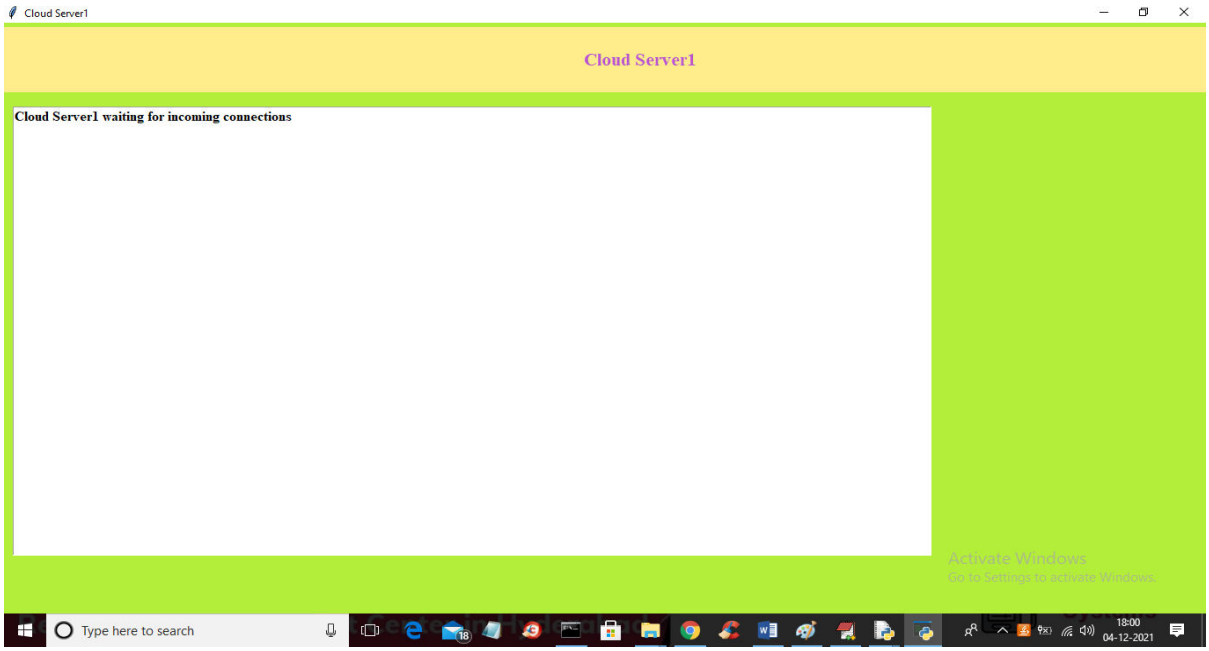
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

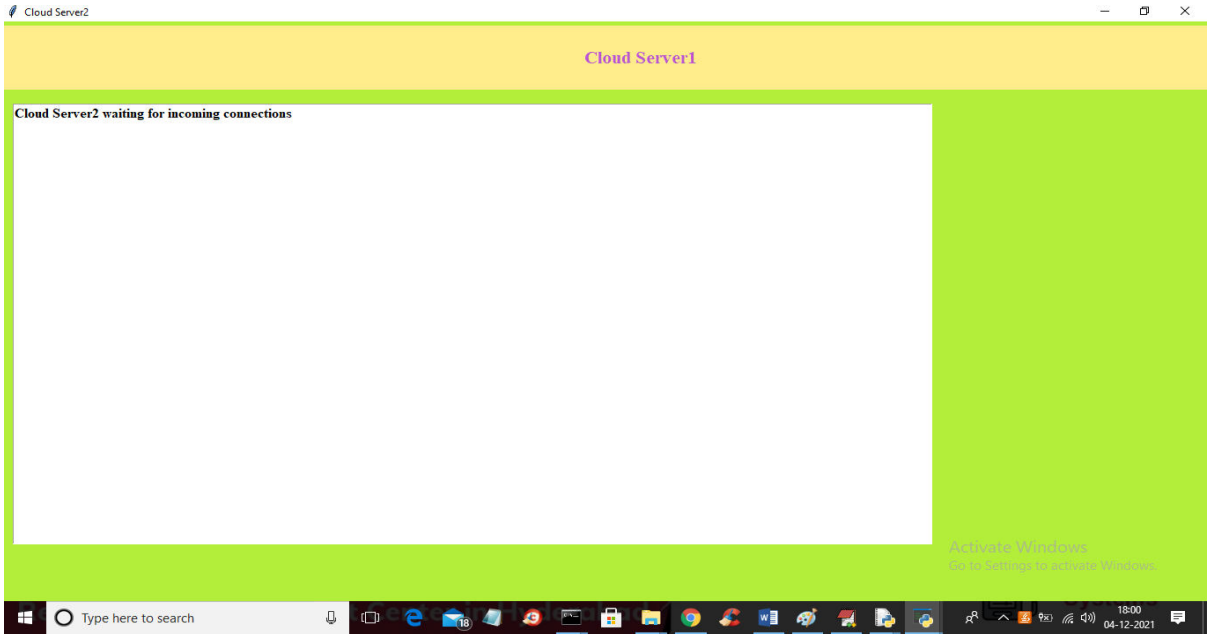
| DOI: 10.15680/IJIRCCE.2024.1203122 |

V. EXPERIMENTAL RESULTS

First run the file from 'CloudServer1' folder to get below screen and to start first cloud server



In above screen cloud server1 started. Now double click on 'run.bat' file from 'CloudServer2' folderto start cloud 2 and to get below screen

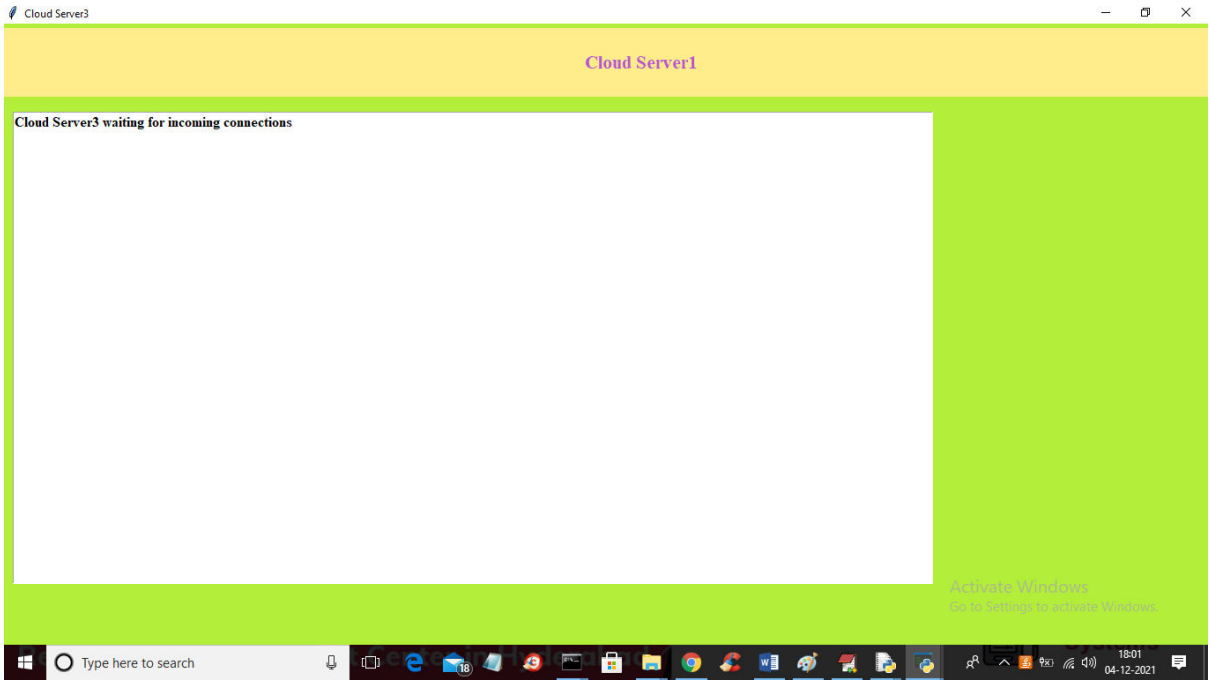


In above screen cloud server2 started. Now double click on 'run.bat' file from 'CloudServer3' folderto start cloud 3 and to get below screen

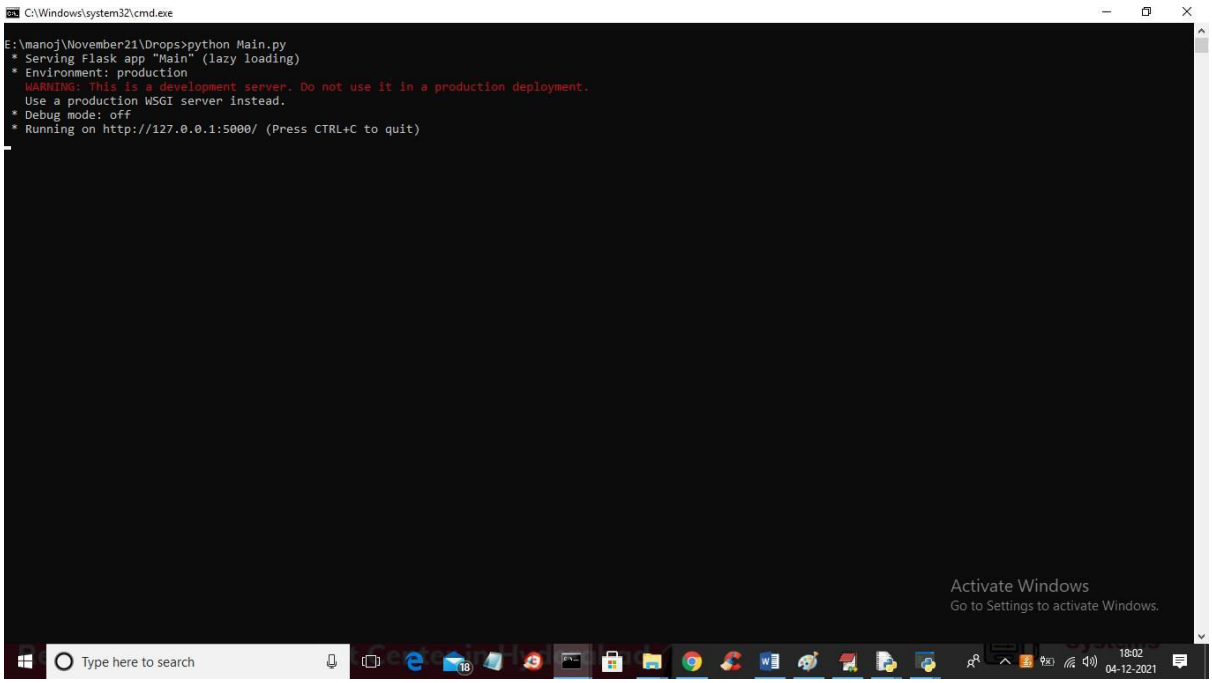
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



In above screen cloud server3 started. Now double Click on 'run.bat' file from 'Drops' main folder tostart python FLASK server and to get below screen

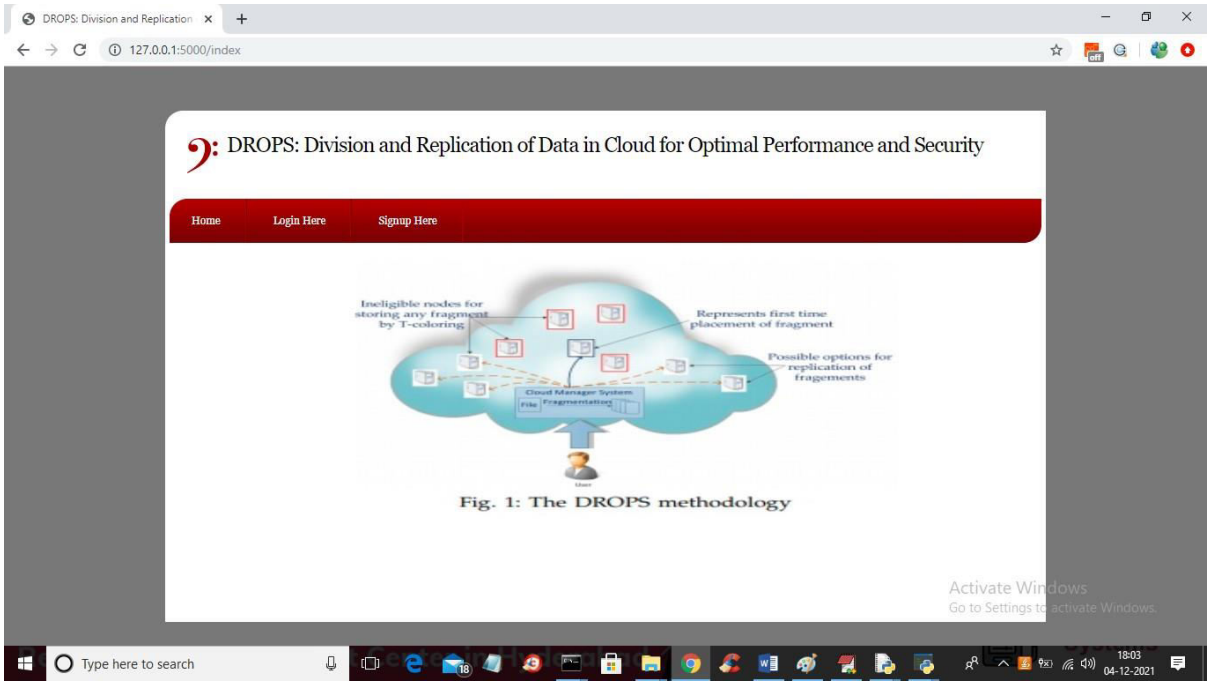


In above screen python server started and now open browser and enter URL as 'http://127.0.0.1:5000/index' and press enter key to get below screen

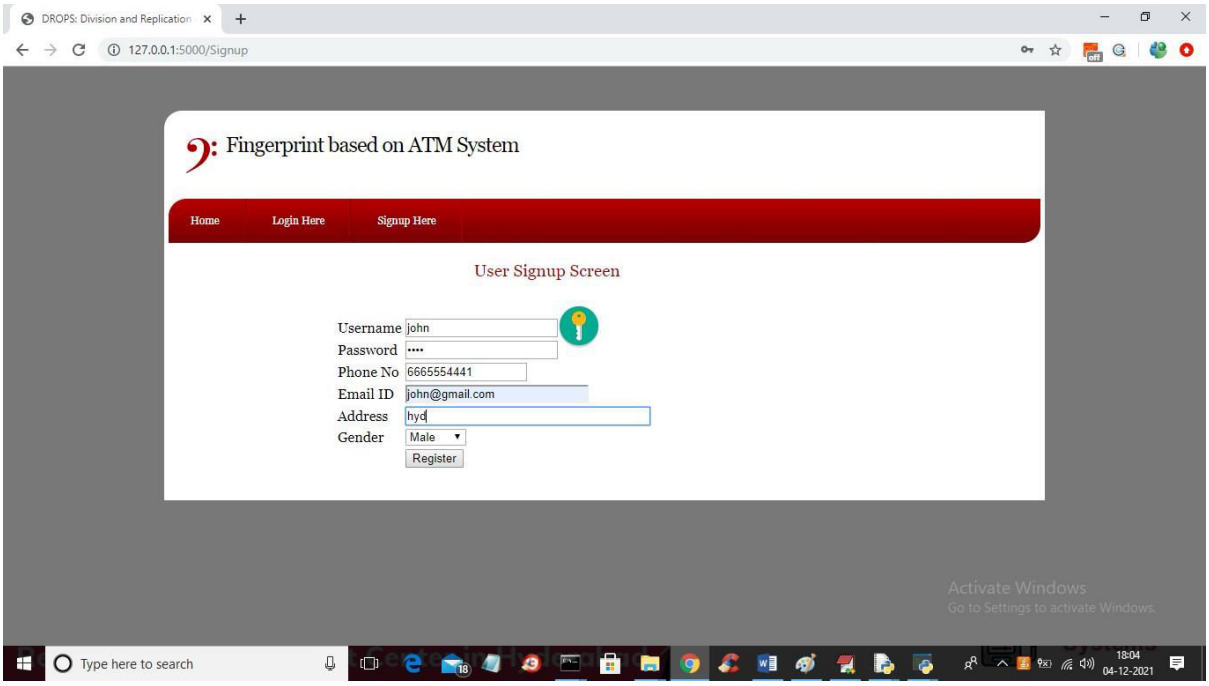
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



Now click on 'Signup Here' link to add new user and to get below screen



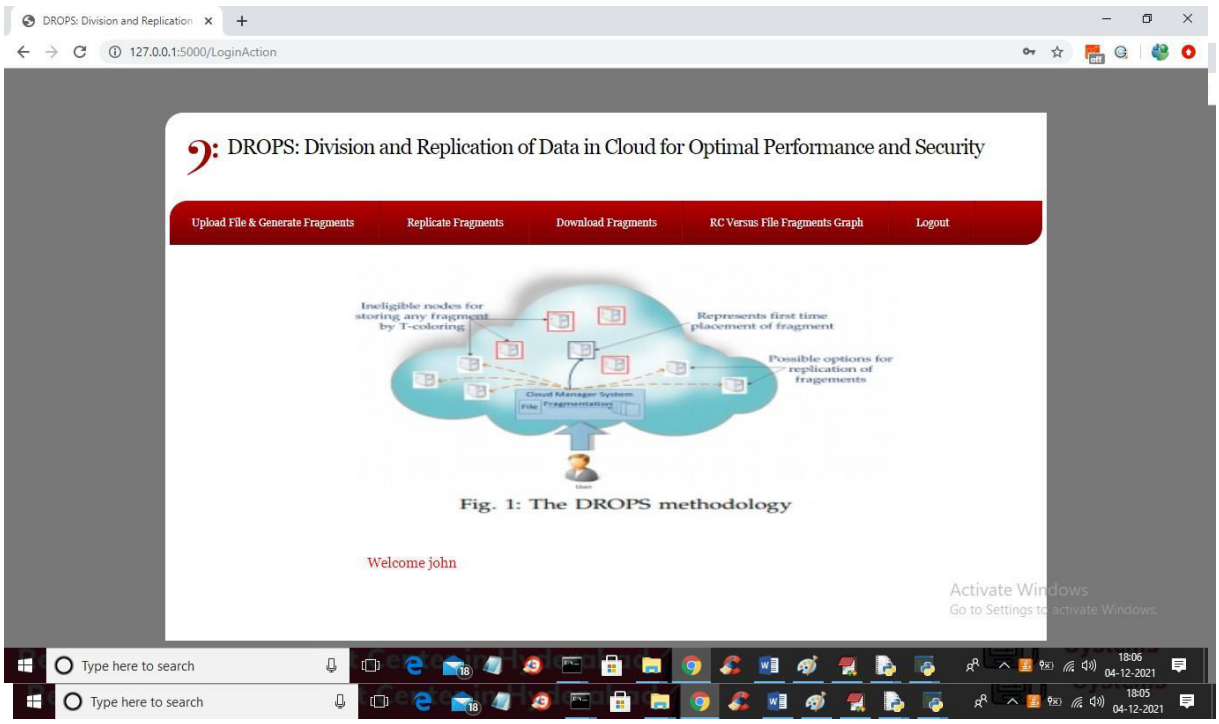
In above screen one user is signing and after signing will get below screen

International Journal of Innovative Research in Computer and Communication Engineering

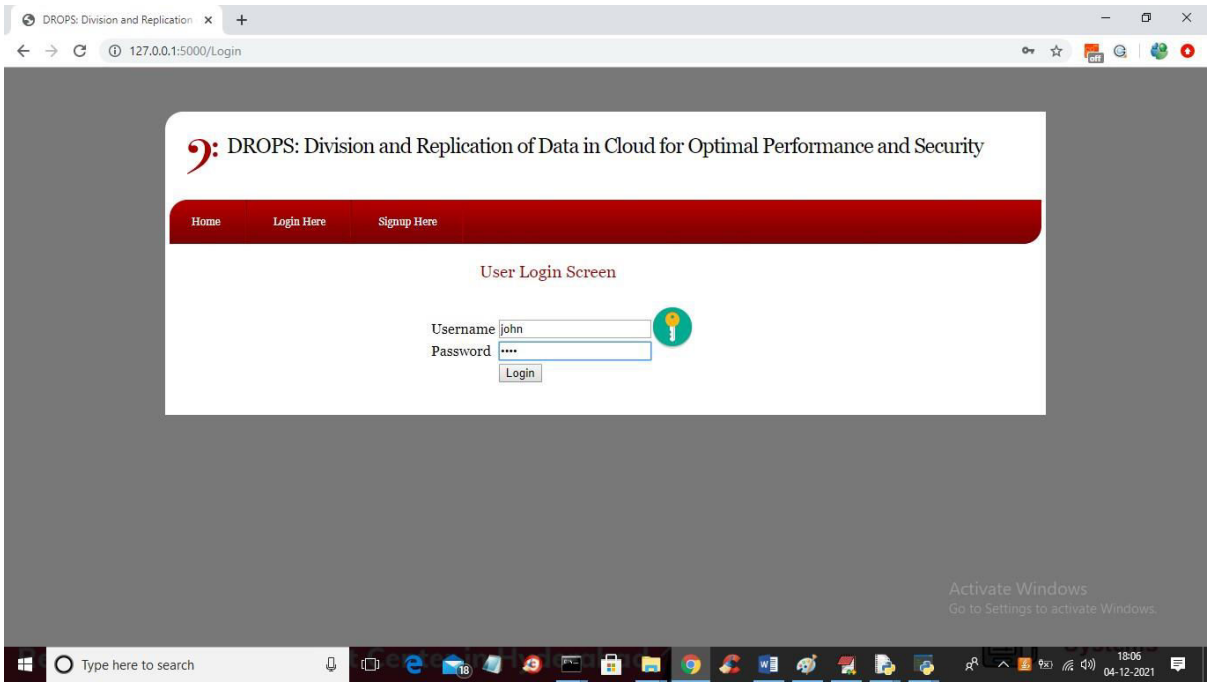
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



In above screen user signup process completed and now click on 'Login Here' link to get below loginscreen



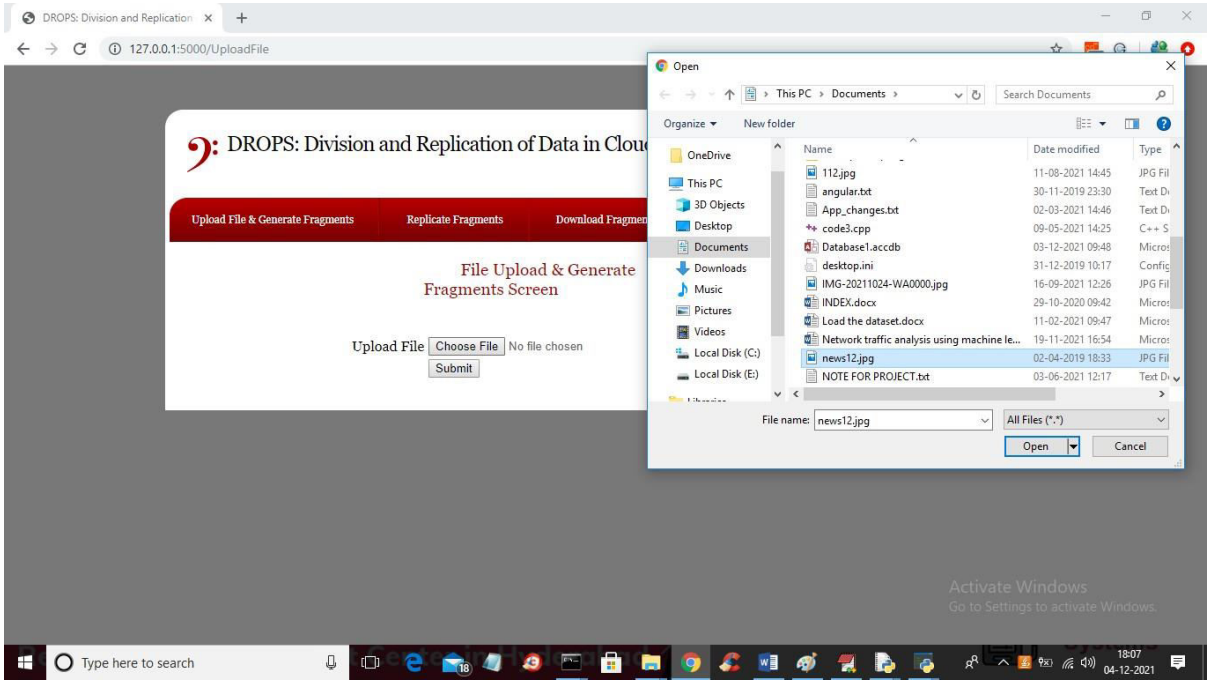
In above screen user is login and after login will get below screen

In above screen click on 'Upload File & Generate Fragments' link to upload file and to get belowscreen

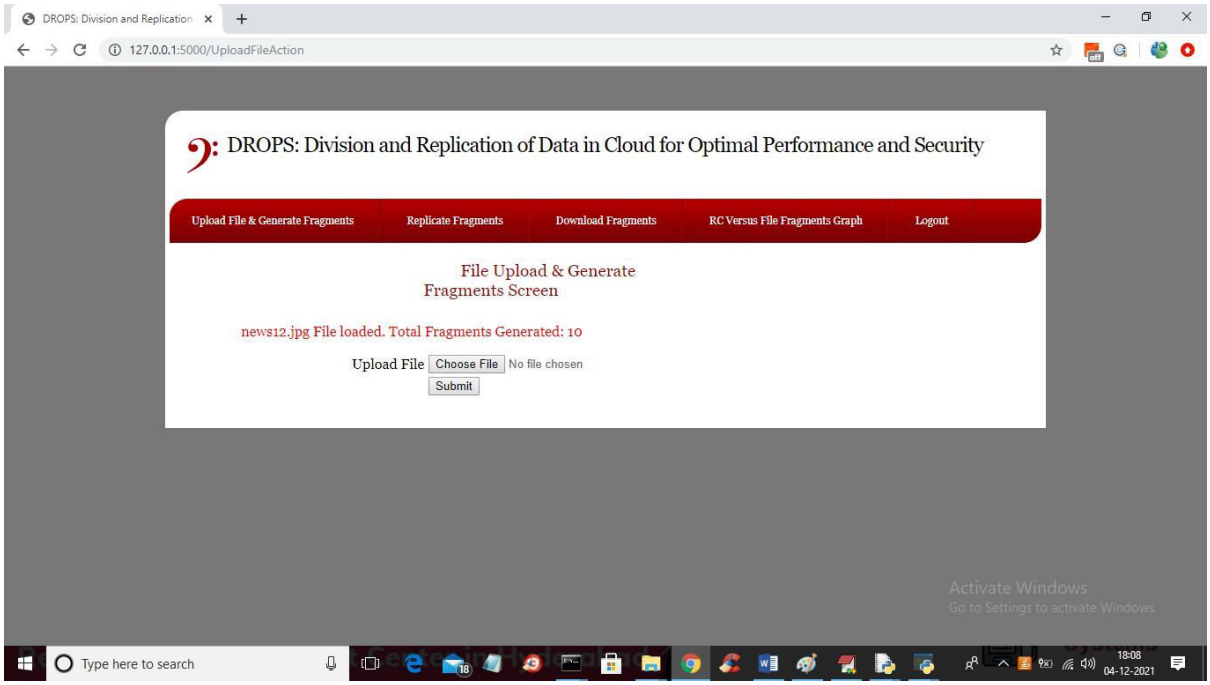
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



In above screen click on 'Choose File' option and then select any type of file to upload and in above Iselected 'news12.jpg' file and then click on 'Open' button to upload file and to generate fragments

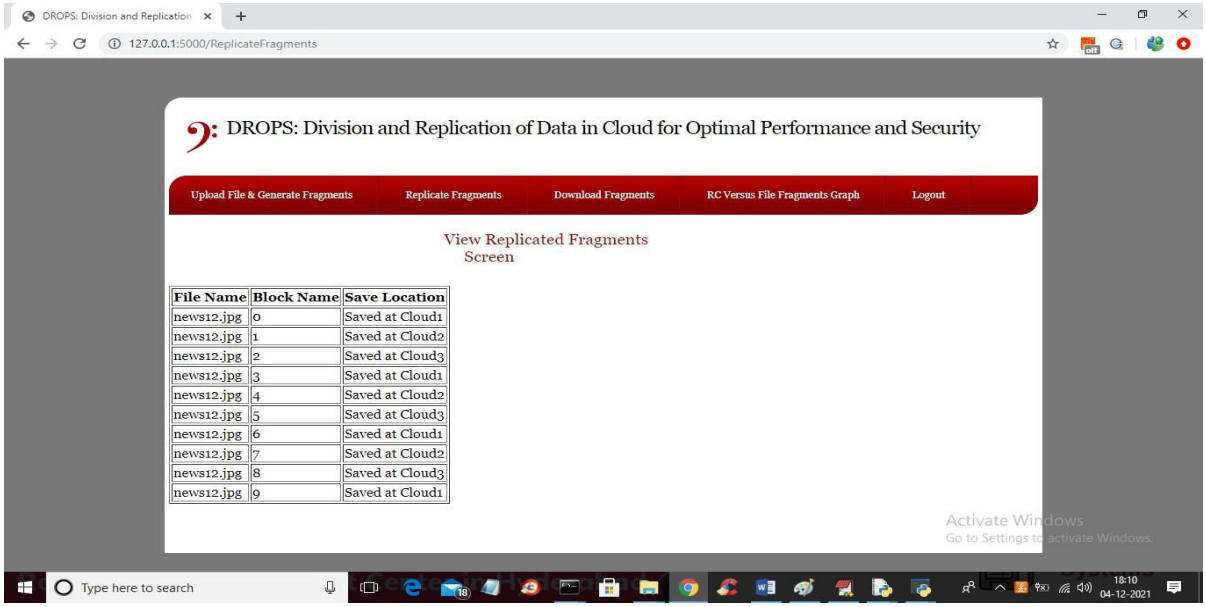


In above screen file uploaded and total 10 fragments generated and now click on 'ReplicateFragments' link to send all fragments to 3 cloud servers and to get below screen

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

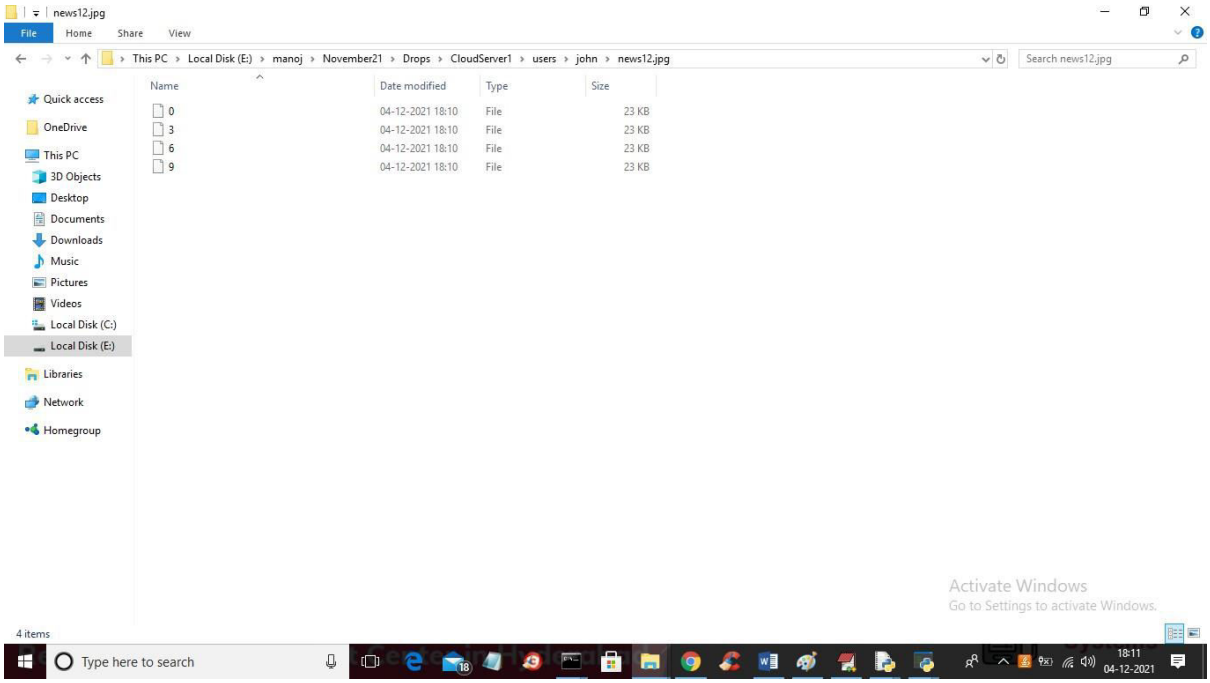
|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



In above screen we can see 10 fragments with file name, block name and cloud server name wherethis fragments is store. In below cloud server1 ‘users’ folder we can see this blocks

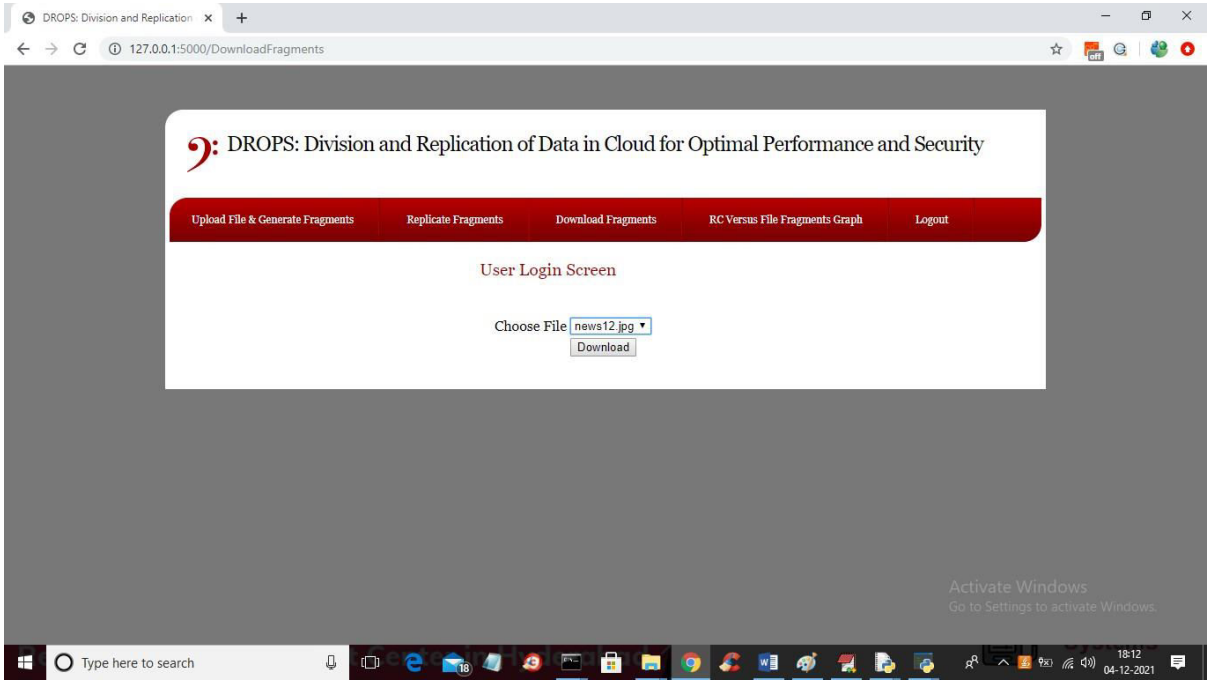
In above screen in cloud server1 under users/john/news12.jpg’ 4 blocks are saved and remaining blocks will be saved at cloud server 2 and 3 and now click on ‘Download Fragments’ link to getbelow screen



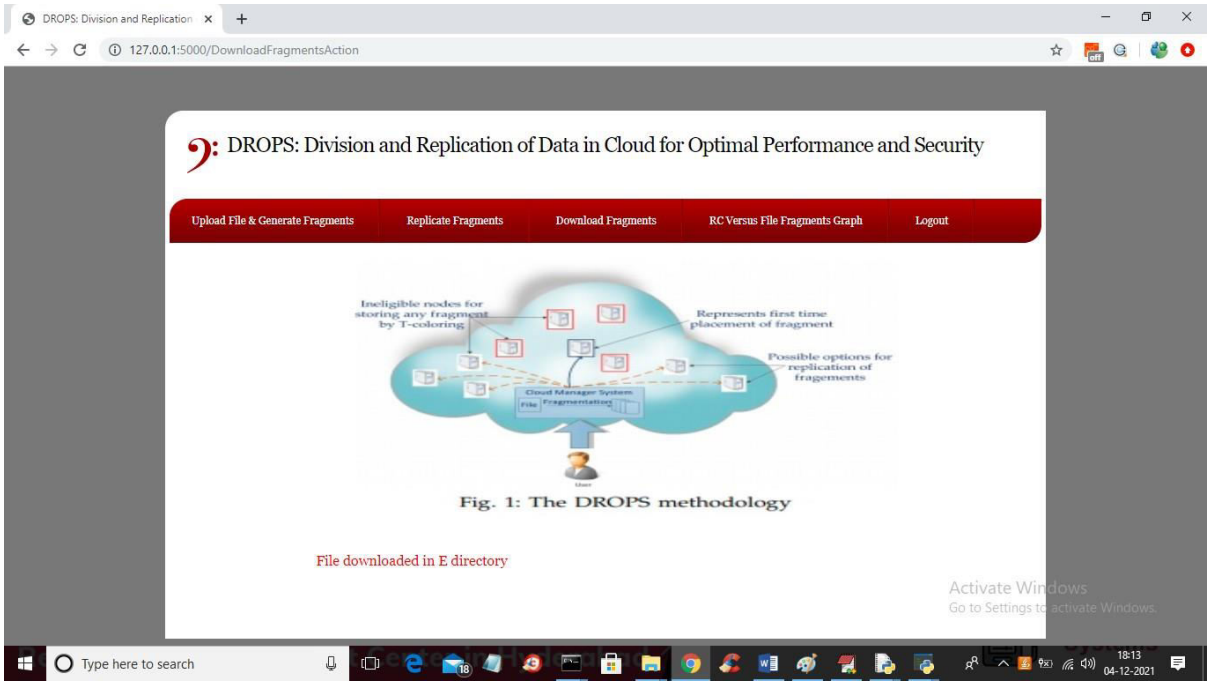
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



In above screen from drop down box user can select any file which is uploaded by and then click on'Download' button to download file



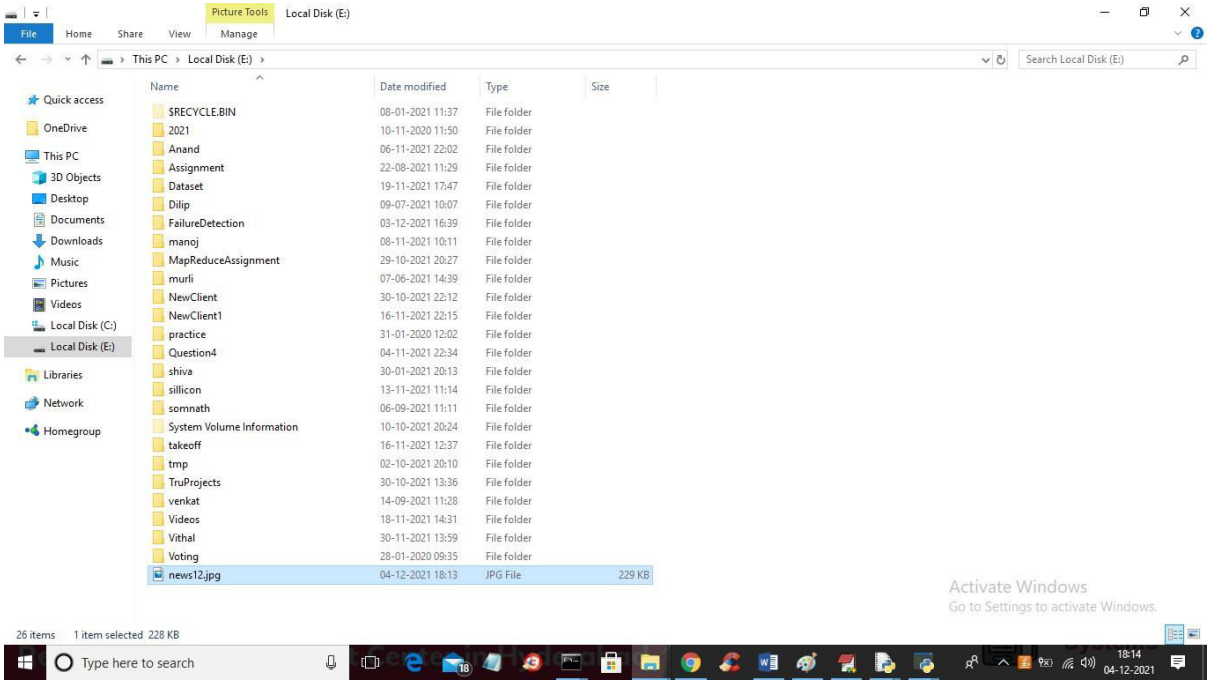
In above screen in red color text we can see file downloaded in E directory and we can see that file inE directory in below screen

International Journal of Innovative Research in Computer and Communication Engineering

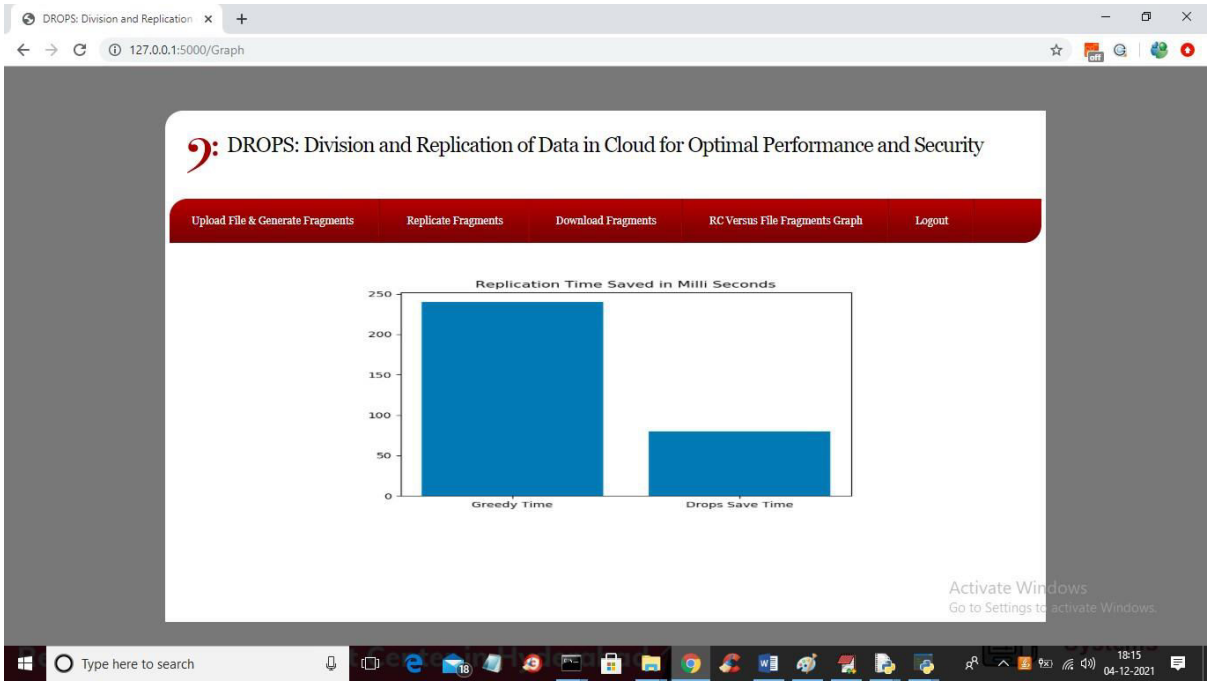
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |



In above screen in E directory in last file we can see news12.jpg file downloaded and now click on 'RC Versus File Fragments Graph' link to get below graph



In above graph x-axis represents algorithm names and y-axis represents block saving time and drop is the propose work which took less time compare to existing Greedy Algorithm. Drop will save storage time by sending blocks/replications to multiple servers

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203122 |

VI. CONCLUSION AND FUTURE WORK

In conclusion, the Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) methodology presents a robust approach to addressing the dual concerns of data security and retrieval performance in cloud computing environments. By dividing files into fragments and strategically replicating them across cloud nodes, DROPS significantly enhances security by minimizing the risk of data compromise in the event of attacks by malicious users or nodes within the cloud. Furthermore, the distance-based separation of nodes storing fragments, achieved through graph T-coloring, adds an additional layer of protection by preventing attackers from easily deducing the locations of fragments, thereby enhancing the overall resilience of the system against potential breaches.

One of the key strengths of the DROPS methodology is its departure from traditional cryptographic techniques for data security. By adopting a novel approach that does not rely on computationally expensive cryptographic algorithms, DROPS reduces the computational burden on the system while still ensuring robust security measures. This not only enhancesthe efficiency of data retrieval but also contributes to the scalability and cost-effectiveness of cloud computing environments.

Moreover, our analysis demonstrates that the probability of locating and compromising all nodes storing fragments of a single file is exceedingly low, further validating the effectiveness of the DROPS methodology in safeguarding sensitive data against potential threats. Additionally, our comparative performance evaluation reveals that DROPS outperforms ten other schemes in terms of security with only a slight overhead on retrieval performance. This highlights the practical viability of DROPS as a security-enhancing solution for cloud computing environments without compromising on performance.

In conclusion, the DROPS methodology presents a compelling solution to the security and performance challenges inherent in cloud computing, offering a balanced approach that prioritizes both data protection and efficient data retrieval. As research in this field continues to evolve, DROPS stands poised to make significant contributions towards fortifying the security posture of cloud-based systems while ensuring optimal performance and scalability.

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 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details