# “An Study on-Cloud Security Using DROPS Technique”

LADE MAYURI S. LOLAGE PRANALI S.
NAGARE MAYURI S. SADAPHAL PRIYANKA V.
Prof. Jorwekar Y.S

## Abstract

*Cloud Computing (CC) is an emerging trend that offers number of important advantages. One of the fundamental advantages of CC is pay-as-per-use, where customers will pay only according to their usage of the services. Outsourcing data to a third-party administrative control, it 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 Cloud Security Using DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security) Technique that collectively approaches the security and performance issues. In the DROPS technique, 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. The DROPS technique does not depend on the traditional cryptographic techniques for the data security; 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 is extremely low. We also compare the performance of the DROPS technique 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 utilized security procedure should likewise consider the improvement of the information recovery time. Cloud Security Using DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security) Technique that aggregately approaches the security and performance issues. In the DROPS technique, we separate a document into sections, and duplicate the divided information over the cloud nodes. 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 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 benefit does not solely depend on an individual’s security measures. The neighbouring entities may provide an opportunity to an attacker to bypass the users defences. 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. Furthermore, 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 may access to unauthorized data. Similarly, cross-tenant virtualized network access may also compromise data privacy and integrity. Due to improper media sanitization can also leak customer’s private data.

## II. EXISTING SYSTEM

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. cross-tenant virtualized network access may also compromise data privacy and integrity. Improper media sanitization can also leak customer's private data. The data must be secured when it is transferred to the public cloud, outside the organizations administrative domain. Accessing the data by the unauthorized users and process should be prevented. Otherwise the weak entity will put the cloud at risk.

## III.LITURATURE SURVEY :

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.
   In this paper, we studied the structural robustness of the state-of-the-art data center network (DCN) architectures. Our results revealed that the DCell architecture degrades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture. Because of the connectivity pattern, layered architecture, and heterogeneous nature of the network, the results demonstrated that the classical robustness metrics are insufficient to quantify the DCN robustness appropriately. Henceforth, signifying and igniting the need for new robustness metrics for the DCN robustness quantification. We proposed deterioration metric to quantify the DCN robustness. The deterioration metric evaluates the network robustness based on the percentage change in the graph structure. The results of the deterioration metric illustrated that the DCell is the most robust architecture among all of the considered DCNs.

2. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing data centers," In IEEE Globecom Workshops, 2013, pp. 446-451.
   This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications. The performance evaluation is carried out using GreenCloud – the simulator focusing on energy efficiency and communication processes in cloud computing data centers. The obtained results confirm that replicating data closer to data consumers, i.e., cloud applications, can reduce energy consumption, bandwidth usage, and communication delays significantly.

3. 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.
   Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

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

In this paper we elucidate cloud computing and major security issues of cloud computing. By utilizing various facilities and services provided by cloud one can increase performance, agility and efficiency in addition to reduce cost and management responsibilities of an enterprise. Though there are lots of advantages of cloud, there are yet numerous challenges to be faced by cloud computing such as privacy issues and data security. In this paper we have tried to address most critical data security challenges of cloud. Many standard organizations such as National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA) and Cloud Computing Interoperability Forum (CCIF) are trying to develop standards to resolve various security issues of cloud. Cloud computing has the potential to provide a secure and economically viable IT solution in the future.

5. 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.
   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.

## IV. PROPOSED SYSTEM

In proposed system, we collectively approach the issue of security and performance as a secure data replication problem. The division of a file into fragments is performed based on a given user criteria. Divided File can store in different nodes. 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.

Security is one of the most crucial aspects among those prohibiting the widespread adoption of cloud computing. Cloud security issues may stem due to the core technologies implementation (virtual machine (VM). The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. The main aim of our project is secure the files store on cloud. The division of a file into fragments is performed based on a given user criteria. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security. We select the nodes in a manner that they are not adjacent and are at certain distance from each other. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.

## V. SYSTEM ARCHITECTURE:-

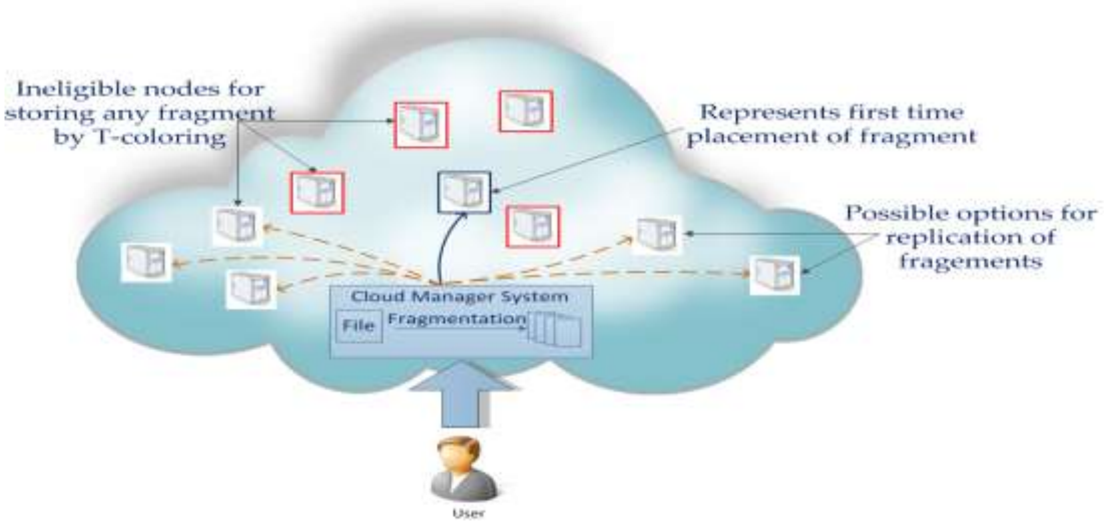
Ineligible nodes for storing any fragment by T-coloring
Represents first time placement of fragment
Possible options for replication of fragements
Cloud Manager System
File
Fragmentation
User

Fig 1. System Architecture

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. 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.

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.

In this system mainly consist of three modules:

- Owner
- User
- Cloud Admin

**Owner-**

In these owner modules, owner add the multiple users in the cloud system. Owner also uploads the text files in the cloud storage. He can delete the files.

**User-**

In user module, user completes the registration process and login the system. He can upload the text files on cloud storage. He can delete, update or modify the files

**Cloud Admin-**

In this module, the views the all status, views user, view owner, and reports send back. The Cloud admin module file can fragments using the fragment placement and fragments replication algorithms

## VI. FUTURE SCOPE

The scope of this project is the DROPS technique; 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.

## VII. CONCLUSION

Division and Replication of Data in Cloud for Optimal Performance and Security (DROPS) use the P-class. P-class of polynomially solvable problems, P contains all sets in which membership may be decided by an algorithm whose running time is bounded by a polynomial. In this project files are fragments and store on each nodes in cloud storage. The output is directly shows.

## REFRENCES:

[1] Bhole Laxmikant, Mrs. M.S haikh, Patil Pratik kumar, Salve Rahul, Warade Pratik :"A SURVEY ON CLOUD DATA ACCESS PRIVILEGE WITH FULLY ATTRIBUTE – BASED ENCRYPTION WITHGEO SOCIAL SECURITY", Vol. 3, Issue 11, November 2015

[2] „DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security" Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj
Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and
Albert Y. Zomaya, Fellow, IEEE

[3] 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.

[4] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, “On the placement of web server replicas,” In Proceed ings of INFOCOM2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1587 - 1596, 2001.
[5] B. Grobauer, T.Walloschek, and E. Stocker, “Understanding cloud computing vulnerabilities,” IEEE Security and Priva cy, Vol.9, No.
2, 2011, pp. 50-57.
[6] 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
[7]M. Newman, Networks: An introduction, Oxford University Press,
2009.
[8]PDDS -Improving Cloud Data Storage SecurityUsing DataPartitioning Technique‟C. SelvakumarDepartment of Information Technology MIT Campus, Anna University Chennai, Tamil Nadu, G. Jeeva Rathanam Department of Information Technology MIT Campus, Anna University Chennai, Tamil Nadu, M. R. Suma latha Department of Information TechnologyMIT Campus, Anna University Chennai, Tamil Nadu.
[9]Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.; "Slicing: A New Approach for Privacy Preserving Data Publishing," Knowledge and Data
Engineering, IEEE Transactions on vol.24, no.3, pp.561- 574, March2012