International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

Analysis of Cloud Security and Performance for Leakage of Critical Information using DROPS Methodology

Monisha Thomas[1], Laxmi Choudhary[2], Indra Kishor [3]

[1,2]B.Tech. Scholars, Dept. Of CSE, Arya Institute of Engineering and Technology, Kukas Jaipur Raj.
[3]Associate Prof. Department of CSE, Arya Institute of Engineering and Technology, Kukas Jaipur Raj.

Abstract - *When outsourcing of data to the third-party administrative control is done in cloud computing then it can cause security concerns or problems. The data may be attacked by other users and nodes within the cloud. So, data must be protected using high security measures within the cloud. Moreover, the security measures must also be concern with the optimization of the data at the retrieval time. In this paper, we propose DROPS methodology that approaches both the security and performance issues. In this methodology, a file is divided into fragments and the fragmented data is replicated over the cloud nodes. Each node stores only a single fragment of a particular data file that ensures no meaningful information is revealed to the attacker in the successful attack. Moreover, the nodes storing the fragments are separated by the certain distance with the help of T-coloring graph to restrict an attacker of guessing the locations of the fragments.*

Key Words: **cloud, division, replication, optimal, security, T-coloring graph, fragmented, performance, node, centrality, outsourcing, critical**

1. INTRODUCTION

Cloud is a representation of the Internet and other communications. The term cloud can be simply defined by how a network or remote servers can be accessed via an internet connection for managing and storing the information. Cloud is a place where user can store all the information in the computer.

DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security) is a methodology that is an approach for both securing and performance issue of the data.[2]

Cloud drops technology is used for securing data over the cloud so that, when the users outsource their data to third party administrative control, it gives rise to security concerns i.e., the data can be attacked by the other users, processes and nodes within the cloud.[5]

Cloud Security can be enhanced using DROPS methodology that improves both the security and performance issues. Security is one of the most important aspects among those restricting the widespread adoption of cloud computing. Cloud security issues may arise 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 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.[2]

2. THREATS AND SECURITY STRATERGIES IN CLOUD COMPUTING

2.1 THREATS

2.1.1 The entity or neighbouring entity may provide the opportunity to an attacker to bypass the user security and may access the user data files.

2.1.2 The off-site data storage cloud utility requires the users to move data in cloud and shared environment that may cause various security concerns and hamper the user data.

2.1.3 In the pooling and elasticity of the cloud the physical resources are shared among many users. These shared resources may be reassigned to other users for some duration of time that may cause the risk to the data.

2.1.4 A multi-tenant virtual environment may result in VM to escape the boundaries of virtual machine monitor (VMM) which can interfere to other VMs may access to unauthorized data.

2.1.5 In cross tenant virtualized network, due to improper media sanitization, the customer data can also get leaked.[4]

2.2 DATA SECURITY STRATERGIES

2.2.1 In the DROPS methodology, a file is divided into fragments, and replicates the fragmented data over the cloud nodes, which is duplicating the data. Each of the nodes stores only a single fragment of a particular data file that ensures that even in the case of a successful attack, no meaningful information is revealed to the attackers [3].

2.2.2 The nodes storing the fragments are separated by a certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

2.2.3 For a cloud to be secured, all participating entities must be secure. In a system with multiple units, the highest

level of systems security is equal to the security level of the weakest entity.[3]

Fig. 1: Cloud storage

3. DROPS METHODOLOGY SYSTEM

In the DROPS methodology 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. [5]

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 of the user data files by other users, processes and nodes must be prevented. The main aim is to secure the files store on cloud. The division of a file into fragments is performed based on a given user criteria and only single replication of the fragment is done. DROPS methodology suggests that successful attack on the single node will not reveal the locations and the important information of other fragments within the cloud. To keep an intruder uncertain about the locations of the file fragments to further improve the security. The selection of the nodes is done 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 [9].

3.1 SYSTEM ARCHITECTURE

The data which is outsourced must be secured so that third party user cannot access the data which is stored in the cloud. Unauthorized access to the data of the user by the other users or process must be denied or prevented. [8]

Any weak entity which is present can risk the whole cloud. In such a case, 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 must also be minimized. Scheme is developed for outsourced data that takes into account both the security and performance.

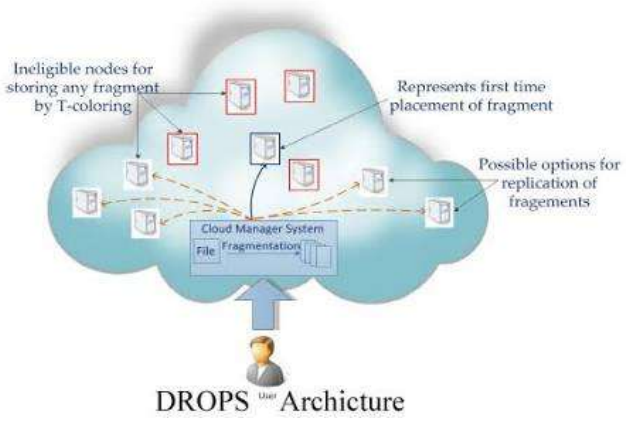

Fig. 2: DROPS Architecture

The DROPS system scheme fragments the user data and replicates the fragmented data or files all over cloud nodes. The proposed DROPS scheme ensures that even in the successful intrusion, no important information is revealed to the attacker. In this paper, the traditional cryptographic techniques for data security is not used as it is slower and does not provide the security required to protect the data from the intruder. The operations (placement and retrieval) on the data are made faster by the help of non-cryptographic nature of the proposed scheme. The controlled replication of the file fragments is ensured and each fragment is replicated only once to improve the security of the data. [6]

The system consists of three modules:

- Owner
- User
- Cloud Admin

- **Owner**- In the owner module, owner can add the multiple users in the cloud system and moreover, can uploads the text files in the cloud storage. The owner can delete the files which is not required.
- **User**- In the user module, user first completely their registration and then login in system. The user can upload the text files, delete, update or modify the files on the cloud storages per the need of the user.
- **Cloud Admin**- In the cloud Admin module, the admin can view users, view owner, view all the status and reports, etc. This modules file can be fragmented using the

different algorithms such as fragment placement and fragment replication algorithms.[7]

CONCLUSIONS

Division and Replication of Data in Cloud for Optimal Performance and Security (DROPS) is used for securing and improving the data which outsourced on the cloud so that no intruder can access the data. The data which is outsourced is divided into the fragments and replicated. The replicated files are sent to the different nodes of the cloud. The node stores only the single fragment of the data files. The fragments are only replicated once so that there is no redundancy of the data and security of the data can be improved using DROPS Methodology.

Division and Replication of Data in Cloud for Optimal Performance and Security (DROPS) use the P-class of polynomial solvable problems. P contains all sets in which membership may be decided by an algorithm whose running time is bounded by a polynomial.

REFERENCES

[1] Bhole Laxmikant, Mrs. M.S haikh, Patil Pratik kumar, Salve Rahul, WaradePratik :||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] 3. T. Loukopoulos and I. Ahmad, —Static and adaptive distributed data replication using genetic algorithms, || Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp.1270-1285.

[4] Bi, X., Grossman, T., Matejka, J., & Fitzmaurice, G.: Magic desk: bringing multi-touch surfaces into desktop work. Proc. CHI ’11.

[5] Dey, A. K. and Guzman, E.: From awareness to connectedness: the design and deployment of presence displays. Proc. CHI '06.

[6] Dourish, P., and Bly, S.: Portholes: supporting awareness in a distributed work group. Proc. CHI’92.

[7] Elliot, K., Neustaedter, C., and Greenberg, S.: StickySpots: using location to embed technology in the social practices of the home. Proc. TEI’07.

[8] B. Grobauer, T.Walloschek, and E. Stocker, —Understanding cloud computing vulnerabilities,|| IEEE Security and Priva cy, Vol.9, No. 2, 2011, pp. 50-57.

[9] 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

ACKNOWELEGMENT

Under the guidance of Mr. Indra Kishor, Associate Prof. Department of CSE, Arya Institute of Engineering and Technology, we analyzed the paper entitled Analysis of cloud Security and performance for leakage of critical information using DROPS Methodology

AUTHOR PROFILE

[1] Mr. Indra Kishor, Associate Prof. Department of CSE, Arya Institute of Engineering and Technology

[2] Monisha Thomas, B.Tech. Scholar, Department of CSE, Arya Institute of Engineering and Technology

[3] Laxmi Choudhary, B.Tech. Scholar, Department of CSE, Arya Institute of Engineering and Technology