An Efficient Detection and Authentication Based On Fragmentation Technique in the Cloud

S.Dhivya
M.Tech Student, Department of Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tamilnadu.

M.Kamala Malar
Assistant Professor, Department of Information Technology, Dr.Sivanthi Aditanar College of Engineering,Tamilnadu

P.Anusuya
M.Tech Student, Department of Information Technology, Dr. Sivanthi Aditanar College of Engineering, Tamilnadu.

Abstract – Security is one of the most crucial aspects among those the wide-spread adoption of cloud computing.The third-party administrative control is done in cloud computing which gives rise to security concerns the attacks may happens by data of other users and nodes within the cloud hence, high security measures are required to protect data within the cloud. In this paper we propose (DROPS) Division and Replication of Data in the Cloud for optimal performance and security.Here the file is fragmented and then replicate the fragmented data over the cloud nodes.The nodes store only a single fragment of a particular data file that ensures even in case of attack no meaningful information is revealed to the attacker.The DROPS methodology is used for providing higher level of security.

Index Terms – Data Fragmentation, Replication, Security.

1. INTRODUCTION

Cloud computing security processes should address the security controls over the cloud provider to secure cloud all of the participating entities must be secure. In a cloud the security of the assets does not solely depend on an individual's security measures because In any given system with multiple units, the highest level of the systems security is equal to the security level of the weakest entity.The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented.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.

The cloud must ensure the throughput,reliabilty and security.In the large scale system the problems of data availabilty and response time are deal with data replication strategy.The security and performance are the major issue in the large scale system.

Each of the cloud nodes (use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. 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. The node separation is ensured by the means of the T-coloring To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. To further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/write requests. The selection of the nodes is performed in two phases in the first phase, the nodes are selected for the initial placement of the fragments based on the centrality measures. In the second phase, the nodes are selected for replication.

In the DROPS methodology, user sends the data file to cloud. The cloud manager system (a user facing server in the cloud that entertains user's requests) upon receiving the file performs: **(**a) fragmentation,**(**b) first cycle of nodes selection and stores one fragment over each of the selected node, and **(**c) second cycle of nodes selection for fragments replication.The cloud manager keeps record of the fragment placement and is assumed to be a secure entity.

2. RELATED WORK

The use of a trusted third party for providing security services in the cloud. The public key infrastructure (PKI) is used to enhance the level of trust in the authentication, integrity, and confidentiality of data and the communication between the involved parties. The keys are generated and managed by the certification authorities. At the user level, the use of temper proof devices, such as smart cards was proposed for the storage of the keys. Similarly,the public key cryptography and trusted third party for providing data security in cloud environments. However, the PKI infrastructure is used to reduce the overheads. The trusted third party is responsible for the generation of public/private keys. The trusted third party may be a single server or multiple servers. The symmetric keys are

protected by combining the public key cryptography and the (k, n) threshold secret sharing schemes. Nevertheless, such schemes do not protect the data files against tempering and loss due to issues arising from virtualization and multi-tenancy. A secure and optimal placement of data objects in a distributed system. An encryption key is divided into n shares and distributed on different sites within the network. The division of a key into n shares is carried out through the threshold secret sharing scheme. The network is divided into clusters. The number of replicas and their placement is determined. A primary site is selected in each of the clusters that allocates the replicas within the cluster. The scheme presented in combines the replication problem with security and access time improvement. Nevertheless, the scheme focuses only on the security of the encryption key. The data files are not fragmented and are handled as a single file. The DROPS methodology, on the other hand, fragments the file and store the fragments on multiple nodes.

The fragmentation threshold of the data file is specified to be generated by the file owner. The file owner can specify the fragmentation threshold in terms of either percentage or the number and size of different fragments. The percentage fragmentation threshold, for instance, can dictate that each fragment will be of 5% size of the total size of the file. Alternatively, the owner may generate a separate file containing information about the fragment number and size, for instance, fragment 1 of size 5,000 Bytes, fragment 2 of size 8,749 Bytes.

3. PROPOSED SYSTEM

In the DROPS methodology,The file doesn't store the entire file at a single node. The DROPS methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even a successful attack on the node leaks no significant information. The DROPS methodology uses replication where each of the fragments is replicated only once in the cloud to improve the security. Although, the controlled replication does not improve the retrieval time it significantly improves the security.

The fragmentation threshold of the data file is specified to be generated by the file owner. The file owner can specify the fragmentation threshold in terms of either percentage or the number and size of different fragments. The percentage fragmentation threshold, for instance, can dictate that each fragment will be of 5% size of the total size of the file.

In Fig1,shows that the Cloud Controller holds the storage of file.The Tenant is the user here each user has Information status,Cloud file access,cloud file sharing.During File sharing the file should be in the encrypted format and then the fragmentation is performed.

Once the file is split into fragments, the DROPS methodology selects the cloud nodes for fragment placement. The selection is made by keeping an equal focus on both security and performance in terms of the access time.The fragmentation is performed on the node that provides the decreased access cost with an objective to improve retrieval time for accessing the fragments for reconstruction of original file. While replicating the fragment, the separation of fragments as explained in the placement technique through Tcoloring

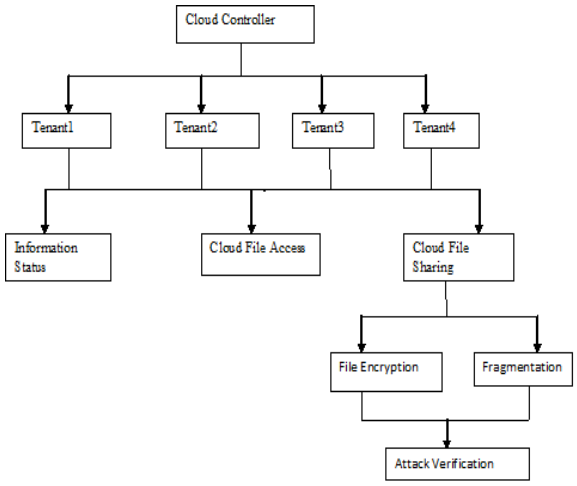

Fig 1 Flow Diagram

4. EXPERIMENTAL RESULTS

In Figure 2, shows that to upload a file the key and privilege should be given

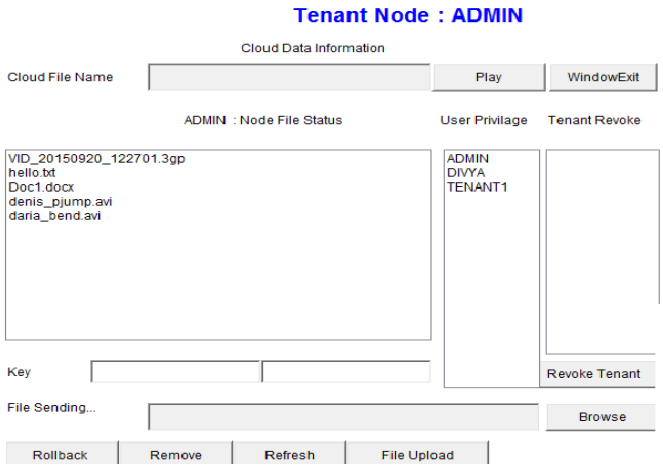

Fig 2 File Uploading

In Figure 3, shows that the file should be accessed by the privilege user

Fig 3 File Accessing

In Figure 4, shows the cloud management system for file

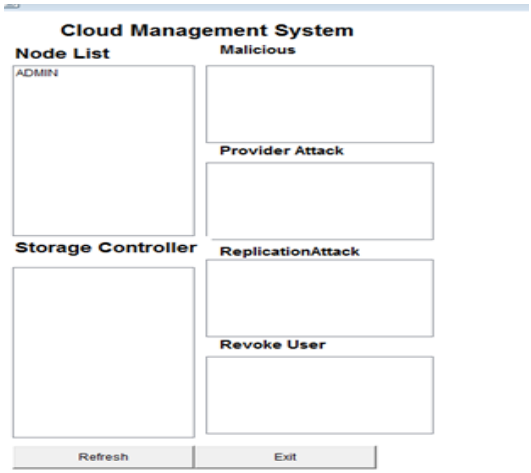

Fig 4 Cloud Controller

5. CONCLUSION

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

REFERENCES

[1] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
[2] W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
[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.
[4] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.
[5] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference on System Sciences (HICSS), 2011, pp. 1-10.
[6] A. Juels and A. Opera, "New approaches to security and availability for cloud data," Communications of the ACM, Vol.56, No. 2, 2013, pp. 64-73.
[7] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583- 592.
[8] J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla,"Selecting the right data distribution scheme for a survivable storage system," Carnegie Mellon University, Technical Report CMU-CS-01- 120, May 2001.
[9] M. Newman, Networks: An introduction, Oxford University Press, 2009.
[10] A. R. Khan, M. Othman, S. A. Madani, S. U. Khan, "A survey of mobile cloud computing application models," IEEE Communications Surveys and Tutorials, DOI:10.1109/SURV.2013.062613.00160.