isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

Data Fragmentation In Cloud For Optimal Performance And Security

G.Priyadharishini[1],A.Sairamya[2] ,Mrs.W.Mercy[3]

Student, Department of Computer Science and Engineering, Agni College of Technology, India

Assistant Professor, Department of Computer Science and Engineering, Agni College of Technology, 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 within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, Data Fragmentation in Cloud for Optimal Performance and Security that collectively approaches the security and performance issues. In this 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, this methodology does not rely 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 this methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

1. INTRODUCTION

The Data Fragmentation 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.No node in the cloud, stored more than a single fragment of the same file.

2 EXISTING SYSTEM

- Cloud security issues may stem due to the core technology's implementation (virtual machine (VM) escape, session riding, etc.), And
- Cloud service offerings (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.)
- 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

3 PROPOSED SYSTEM

- Data Fragmentation in Cloud for Optimal Performance and Security that collectively approaches the security and performance issues.
- 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 probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low.
- In our project, we collectively approach the issue of security and performance as a secure data replication problem. We present Data Fragmentation in Cloud for Optimal Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.
- 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.

4 SYSTEM IMPLEMENTATION

4.1 Develop Cloud Manager System.

The communicational backbone of cloud computing is the Data Centre Network (DCN). We use the Microsoft Azure Cloud Architecture to evaluate the performance of our scheme on legacy as well as state of the art architectures. We developing an Azure cloud

based web application along with corresponding to create multiple nodes in different regions. The managers have all rights about system scalability and update size of the nodes. And also can manage user activities and restrictions. Users need to register account with valid email address. User need to verifying identities for avoiding Sybil or anonymous attackers. Users can upload there any kind of files and can also Downloadable. User can use cloud like a File System basic.

4.2 T-coloring and Fragmentations.

In this methodology, we propose not to store the entire file at a single node. This 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. This methodology uses controlled 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 to the level of full-scale replication, it significantly improves the security.

4.3 Requesting and Replication and Downloading Files.

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: fragmentation, first cycle of nodes selection and stores one fragment over each of the selected node, and 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. To handle the download request from user, the cloud manager collects all the fragments from the nodes and re-assembles them into a single file. Afterwards, the file is sent to the user. User can download a file on users dashboard show option that file can downloadable. And every downloaded file requests and sent requests are stored in cloud manager server. Request will be subject to changed during the process of DROPS methodology.

5 ARCHITECTURE DIAGRAM

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

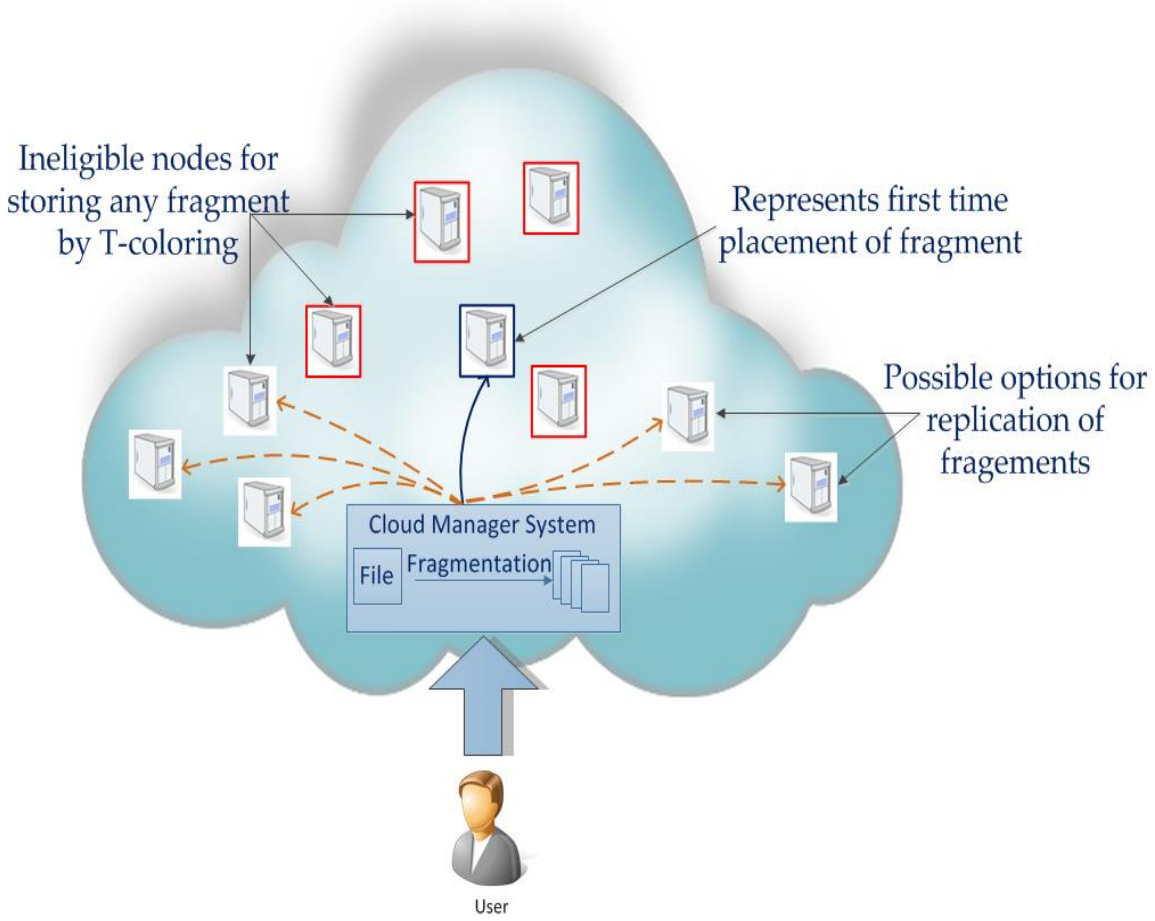

Figure 1: Architecture Diagram.

Figure 1 represents the Data Fragmentation in Cloud for Optimal Performance and Security.User login to Cloud Manager,gets an account verification for the login.File is upload in Drive where the Cloud Manager fragments the file using T – coloring Approach and the file is replicated.User sends Request for Download,Cloud Manager Downloads the data and sends them to the User.

6 CONCLUSIONS

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. 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. The results of

the simulations revealed that the simultaneous focu on the security and performance, resulted in increased security level of data accompanied by a slight performance drop.

7 FUTURE ENHANCEMENTS

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, up- dating, and uploading the file again. Moreover, the implications of TCP incast over the DROPS method- ology 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 data center architectures," Concurrency and Computation: Practice and Experience, 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 robustness of 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, Oakland CA, pp. 110-121, 1991.

[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. 1497-1514.

[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.

[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.

[9] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10. [10] 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.