DROPS: DIVISION AND REPLICATION OF DATA IN CLOUD FOR OPTIMAL PERFORMANCE AND SECURITY

B. Uma Maheswari[1], K. Chandra Sekhar[2]

[1]Assistant Professor, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

[2]PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, 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, 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 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 methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

1. 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 net- work 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 ser- vice offerings (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, In- ternet protocol vulnerability, etc.) [5]. 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 [12]. Therefore, in a cloud, the security of the assets does not solely depend on an individual's security measures [5]. 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 envi- ronment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physi- cal resources to be shared among many users [22]. Moreover, the shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery method- ologies [22]. 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 unau- thorized data [9]. Similarly, cross-tenant virtualized network access may also compromise data privacy and integrity. Improper media sanitization can also leak customer′s private data [5].

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 [14]. 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.

2. LITERATURE SURVEY

Juels et al. [10] 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 and 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. The proposed technique in [10] heavily depends on the user s em- ployed scheme for data confidentiality. Moreover, the probable amount of loss in case of data tempering as a result of intrusion or access by other VMs cannot be decreased. Our proposed strategy does not depend on the traditional cryptographic techniques for data security. Moreover, the DROPS methodology does not store the whole file on a single node to avoid compromise of all of the data in case of successful attack on the node.

The authors in [11] 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. The proposed system is designed and works for object based file systems. However, the leakage of critical information in case of improper sanitization and malicious VM is not han- dled. The DROPS methodology handles the leakage of critical information by fragmenting data file and using multiple nodes to store a single file.

The use of a trusted third party for providing security services in the cloud is advocated in [22]. The authors used the public key infrastructure (PKI) to en- hance 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, Tang et. al. have utilized the public key cryptography and trusted third party for providing data security in cloud environments [20]. However, the authors in [20] have not used the PKI infrastruc- ture to reduce the overheads. The trusted third party is responsible for the generation and management 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 cryptogra- phy 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. n shares is carried out through the (k, n) threshold secret sharing scheme. The network is divided into clusters. The number of replicas and their placement is determined through heuristics. A primary site is selected in each of the clusters that allocates the repli- cas within the cluster. The scheme presented in [21] 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. Moreover, the DROPS methodology focuses on the security of the data within the cloud computing domain that is not considered in [21].

3. PROPOSED SYSTEM

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 andretrieval) 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.

Data Fragmentation

A secure and optimal placement of data objects in a distributed system is presented in [21]. Will require the effort to penetrate only a single node. The amount of compromised data can be reduced by making fragments of

a data file and storing them on separate nodes [17, 21]. A successful intrusion on a single or few nodes will only provide access to a portion of data that might not be of any significance. Moreover, if an attacker is uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very low. Let us consider a cloud with M nodes and a file with z number of fragments. Let s be the number of successful intrusions on distinct nodes, such that s>z.

Homogenous systems, the same flaw can be utilized to target other nodes within the system. The success of an attack on the subsequent nodes will require less effort as compared to the effort on the first node. Comparatively, more effort is required for heterogeneous systems.

However, compromising a single file

a. Betweenness Centrality

The betweenness centrality of a node n is the number of the shortest paths, between other nodes, passing through n [24]. Formally, the betweenness centrality of any node v in a network.

b. Eccentricity

The eccentricity of a node n is the maximum distance to any node from a node n [24]. A node is more central in the network, if it is less eccentric. Formally, the eccentricity can be given as:

The security of a large-scale system, such as cloud depends on the security of the system as a whole and the security of individual nodes. A successful intrusion into a single node may have severe consequences, not only for data and applications on

Centrality

The centrality of a node in a graph provides the measure of the relative importance of a node in the network. The objective of improved retrieval time in replication makes the centrality measures more important. There are various centrality measures; for instance, closeness centrality, degree centrality, betweenness centrality, eccentricity centrality, and eigenvector centrality. We only elaborate on the closeness, betweenness, and eccentricity centralities because we are using the aforesaid three centralities in this work. For the remainder of the centralities, we encourage the readers to review [24].

4. CONCLUSION

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 methodology need to be studied that is relevant to distributed data storage and access. 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 focus on the security and performance, resulted in increased security level of data accompanied by a slight performance drop.

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.

5. 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, pp. 1771-1783, 2013.

[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, pp. 64-77, 2013.

[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 dis- tributed 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, pp. 50-57, 2011.

[6] W. K. Hale, “Frequency assignment: Theory and applications,” Proceedings of the IEEE, vol. 68, no. 12, pp. 1497-1514, 1980.

[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, pp. 1-13, 2013.

[8] M. Hogan, F. Liu, A. Sokol, and J. Tong, NIST Cloud Computing Standards Roadmap, NIST Special Publication, 2011.

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

[10] A. Juels and A. Opera, “New approaches to security and availability for cloud data,” Communications of the ACM, vol. 56, no. 2, pp. 64- 73, 2013.

[11] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, “Dike: Virtualization-aware Access Control for Multitenant File systems,” University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[12] L. M. Kaufman, “Data security in the world of cloud computing,”

IEEE Security and Privacy, vol. 7, no. 4, pp. 61-64, 2009.

[13] S. U. Khan, and I. Ahmad, “Comparison and analysis of ten static heuristics-based internet data replication techniques,” Journal of Parallel and Distributed Computing, vol. 68, no. 2, pp. 113-136, 2008.

[14] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, “Towards secure mobile cloud computing: A survey,” Future Generation Computer Systems, vol. 29, no. 5, pp. 1278, 2013

[15] A. N. Khan, M. L. M. Kiah, S. A. Madani, and M. Ali, “Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing,” The Journal of Supercomputing, vol. 66, no. 3, pp. 1687-1706, 2013.

[16] T. Loukopoulos and I. Ahmad, “Static and adaptive distributed data replication using genetic algorithms,” Journal of Parallel and Distributed Computing, vol. 64, no. 11, pp. 1270-1285, 2004.

[17] 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, pp. 885-896, 2003.

[18] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, “On the placement of web server replicas,” In Proceedings of INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1587-1596, 2001.

[19] D. Sun, G. Chang, L. Sun, and X. Wang, “Surveying and analyzing security, privacy and trust issues in cloud computing environments,” Procedia Engineering, vol. 15, pp. 2852-2856, 2011.

AUTHOR'S PROFILE

B. UMA MAHESWARI is currently working as Assistant Professor in Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.

K. CHANDRA SEKHAR is pursuing MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.