International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

An Effective Security Scheme Using Division and Replication of Data in Cloud for Optimal Performance

Pranjali Bhingarkar[1], Dr. Mohd Shafi Pathan[2]

[1]Savitribai Phule University, SKNCOE, Pune, India
[2]SKNCOE, Savitribai Phule University, Pune, India

Abstract: ***Cloud computing consist of three main parties; service/application provider, third-party which provides resources and the users. Different users put lots of confidential data while using the services and applications on the resources which are manage by third party administrators. Collected data needs security from hackers and from other users using the same service/application and third party administrators. It becomes utmost important that the confidentiality of data is maintain throughout the life cycle. Hence security is the most important aspect of cloud computing. Division and replication methodologies can be used for enhancing security without the cost of performance in cloud computing. These technologies divide the file into number of fragments and these fragments get replicated to different nodes on cloud depending on security level selected by user. Each node contains only single fragment so even in case of successful attack hacker will not receive meaningful information. Nodes on the cloud which stores the fragment are separated by certain distance using T-coloring. DROP handles Authentication attack, Data Recovery attack, Cross VM attack & VM rollback attack. Division and replication methodologies do not rely on encryption/decryption.***

Keywords: Cloud Computing, Security, Performance, Fragmentation, Replication

1. Introduction

Cloud computing is widely used in organizations because of its characteristics like rapid elasticity, measured service, resource pooling, broad network access, on demand self service. While using services, different users put lots of data on resources which are shared with other users. As these resources are on cloud there may be chances of unauthorized users trying to access the data. As the volume of data is very high, acceptable retrieval time becomes another requirement. In this scenario data reliability, integrity and availability are the success factors for the service/application provider and resource provider. To achieve the above success factors we need robust architecture of cloud computing. Important characteristics of cloud architecture are security and scalability. For cloud to be secured all entities need to be secure like week entity as well as strong entities. Using pooling and elasticity of cloud many resources are shared among different users, that user again reshare those resources to other user and so on... This leads to the data privacy problem. There are types of cloud private cloud, public cloud. Private cloud is comparatively secure, but outsourced data to public cloud must be secure. For data security if we use traditional methodologies like cryptography. Performance of system will be down as the number of data is very large to outsource on cloud.

Mostly in industries single node containing the LDAB database which stores authentication information is hack, in this case this is serious issue, in this paper we are proposing to store the password in file which will be fragmented and stored it in encrypted format using AES algorithm.

May 12th 2017 saw the biggest ever attack in internet history "Ransomware ". This virus takes all important data from your computer and encrypts it and asks for money to releasing the data back. DROP will be effective solution for this type of problem. As we are proposing not to store data on single node and divide it into fragments, and store it on node such that one node should contain only one fragment. In such arrangement even one node is attacked the data is not compromised and is available for the user. At the end data will be secure. Nodes on the cloud which stores the fragment are separated by certain distance using graph T-coloring prohibits the attacker to guess the location of fragments. Node selection will be based on the criteria that they are not adjacent to each other. Using graph T-coloring we can ensure this. Node selection is done in two phases:

- For the initial placement of the fragments nodes are selected based on the centrality measures.
- For replication the nodes are selected such that adjacent node does not contain any fragment.

A cloud must ensure throughput, ensuring quality and security. A key component deciding the throughput of a cloud that stores data is the data recuperation time.

2. Review of Literature Survey

Especially, possible administration security malice is taken into account. Few intensions of distributed systems can be designed to tolerate intrusions. In specific application function such as file management and security function such as user authorization and authentication [2]

D. Boru et. al. described the technique of energy efficient replication in paper Energy-efficient data replication in cloud computing data centres Different risks and threats in Cloud Computing and vulnerabilities of cloud system are detailed out in Cloud computing vulnerabilities[3] and An analysis of security issues for cloud computing [4]

Cloud hooks: Security and privacy issues in cloud computing talks about the security, privacy and trust aspects with regards to cloud computing [5]. Replication can be used for enhancing the security in cloud computing as described by authors Manghui Tu and others.

The problem, to ensure the freshness, integrity and availability of the data within the cloud is by making use of the cryptographic techniques. The technique depends on the authentication scheme in order to provide the confidentiality of the data. Here the file blocks are stored in the various levels of the tree [6].

The problem is the secure and optimal placement of data objects over distributive system within the network. Once the encryption key is divided into n shares and is distributed on different sites. The scheme (k, n) threshold secret sharing scheme is used to divide the key into n shares. The network can be divided into clusters. In every cluster, a primary site is selected which allocates the replicas in it. The scheme used here will combines the problem replication along with the security and improve the access time. This scheme focuses on providing the security to the encryption key. The fragmentation of the data files is not done and handles only single file [17].

Placement of Secure Data Objects over Internet Cloud provides different service models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). These models are described in Addressing cloud computing security issues by Dimitrios Zissis, Dimitrios Lekkas [18] In cloud computing, outsourcing data to a third-party administrative control is done, Due to outsourcing security concerns increases. Due to attacks by other users the data compromise may occur. Therefore to protect data within the cloud.

The security and optimal placement of data is done through the fragmentation and as well as the data objects replication. The fragmented file is encrypted and is stored within the network in a distributed fashion. In order for the increased availability of the data, replication is performed in a random manner [13]

3. System Architecture

For a large-scale system's security; such as cloud, depends on the security of the system and the security of individual nodes. So the problem of secure data replication should be approached by considering performance and security collectively. Based on a user's given criteria, the file is divided into fragments depending upon the security level, such that fragments should not include any meaningful information. The data files fragmentation threshold is selected by the file owner. The fragmentation threshold is specified by the file owner in terms of number and size of the different fragments i.e security levels. Every node within the cloud holds only one fragment of same file to raise the security of the data. After all there is the possibility of an effective attack on any node. To keep an attacker unsure about the fragments location and also to improve security, the selection of nodes should be done in such a manner that they should not be adjacent and must be at the certain distance from each other. The separation of the nodes is ensured by using Tcoloring. The fragments are replicated over the nodes to improve the retrieval time. The nodes are selected in two stages. In first stage, initial placement of fragments is done on different nodes based on T-coloring. In second stage, replication of the fragments is done by selecting remaining nodes. At the same time T-coloring ensures adjacent nodes does not contain origina or replicated fragments.

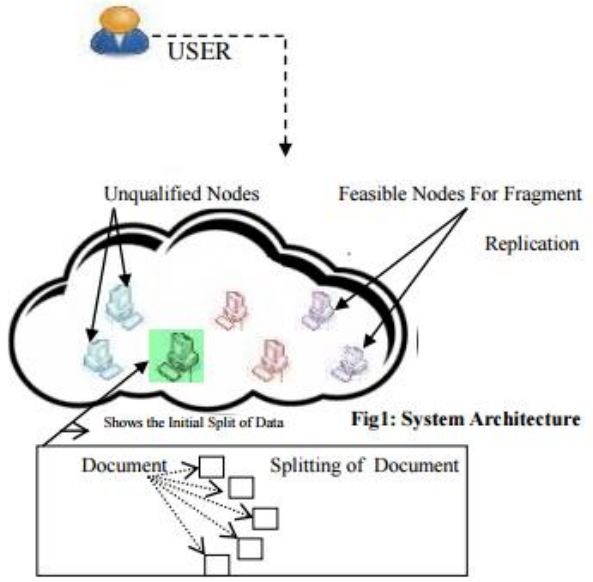

Fig1: System Architecture

For example, File will get fragmented into no of fragments depended upon security level selected by owner of file. The file is best split by the owner such that each fragment should not contain important information as the owner is aware of the facts that pertaining to the data.

4. Methodology

To provide the security to the data file within the cloud the entire file is not stored on a single node. The DROPS methodology is used to fragment the file and replicate over the cloud. The fragments should be distributed such that a node must store a single fragment. In order to improve the security within the cloud, the controlled separation is used by the DROPS methodology in which every fragment is replicated only once. In this methodology, the users need to send the data file to the cloud. Once receiving the data file, the cloud manager system will perform the fragmentation, then selects the node for storing the particular fragment and then replicates the fragments.

Fragment Placement Algorithm:

$A = \{A1, A2 \ldots A_N\}$

$a = \{SIZE\ OF\ (A1), SIZE\ OF\ (A2) \ldots \ldots SIZE\ OF\ (A_N)\}$

$COL = \{OPEN\_COLOR, CLOSE\_COLOR\}$

$CEN = \{CEN1, CEN2, \ldots \ldots \ldots \ldots \ldots CEN_M\}$

$COL \leftarrow OPEN\_COLOR\ FOR\ ALL\ i$

CEN←CEN$_i$ FOR ALL i

COMPUTE:-

FOR EACH A_k BELONGS TO A DO

SELECT P^i/P^i←INDEX OF (MAXIMUM (CEN$_i$))

IF COL s^i = OPEN_COLOR AND pi > = a_k THEN

$P^i \leftarrow A_k$

$p_i \leftarrow p_i - a_k$

$COLs^i \leftarrow$ CLOSE_COLOR

$P^{i'} \leftarrow$ DISTANCE (P^i,T)

$COL_P{}^i \leftarrow$ CLOSE_COLOR

END IF

END FOR

5. Results and Discussions

Objective of DROP is to improve the security. In traditional systems encryption decryption technique were used for data security, where all data is stored on single node which is easy to hack for hacker. For increasing security DROP used fragmentation and replication technique. DROP fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we 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 further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/write requests.

May 12th 2017 saw the biggest ever attack in internet history "Ransomware ". This virus takes all important data from your computer and encrypts it and asks for money to releasing the data back. DROP will be effective solution for this type of problem. As we are proposing not to store data on single node and divide it into fragments, and store it on node such that one node should contain only one fragment. In such arrangement even one node is attacked the data is not compromised and is available for the user. At the end data will be secure. Nodes on the cloud which stores the fragment are separated by certain distance using graph T-coloring prohibits the attacker to guess the location of fragments.

Lets us discussed various attacks which can be chandelled by DROPS methodology.

1. Authentication attack: Node containing the authentication information is hack. Example, consider node containing the LDAB database which contains authentication information is hack, in this case this is serious issue, in this paper we are proposing to store the password in file which will be fragmented and stored it in encrypted format using AES algorithm.

2. Data Recovery: Rollback of VM to some previous state may expose previously stored data. In case a VM is rolled back to a previous state it may start showing the data that is deleted by the user, in the conventional methodology as the entire file is stored on a single node meaningful information is available. But in DROP one node contains only one fragment and that is why even if the data is available it will not be meaningful.

3. Cross VM attack: A malicious VM attacking co resident VM that may lead to data breach. As T-coloring algorithm in DROPS ensures that the fragments are not store on adjacent node cross VM attack will not lead to leaking of meaningful information.

4. E-discovery: Data exposure of one user due to seized hardware for investigations related to some other users.

In DROPS we are storing data in n no of fragments, so E-discovery attack will not lead to leaking of information.

Below Figure1 shows how Fragments of the data file stored on different nodes with T-color to provide security.

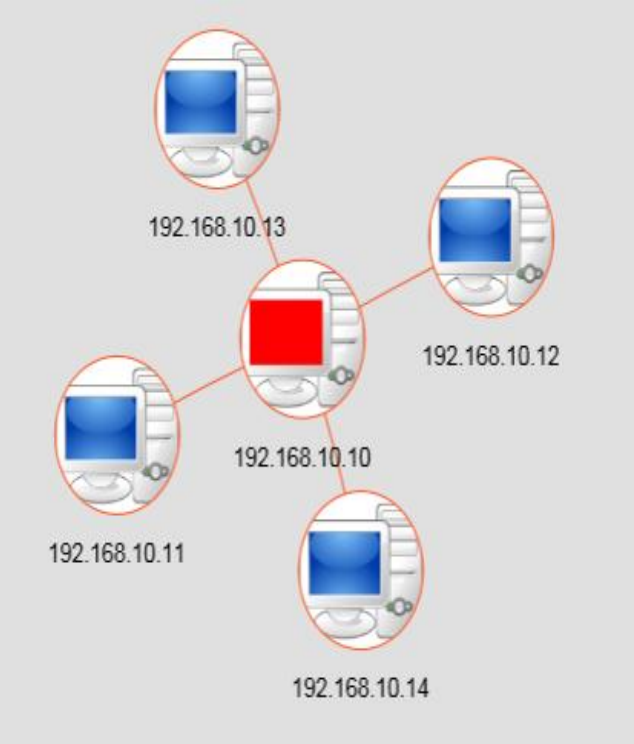

Figure 1: Fragments of the data file stored on different nodes with T-color to provide security.

References

[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.
[2] 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.
[3] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
[4] 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.
[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] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant Filesystems," University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.
[8] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.
[9] 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, 2008, pp. 113-136.
[10] 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, 2013, pp. 1278- 1299.
[11] 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, 2013, pp. 1687- 1706.
[12] 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.
[13] 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
[14] 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.
[15] 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, 2011, pp. 2852 2856.
[16] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, Nov. 2012, pp. 903-916.
[17] M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, "On the optimal placement of secure data objects over Internet," In Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, pp. 14-14, 2005.
[18] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.
[19] 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.
[20] 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.
[21] Xun Yi, San Ling, and Huaxiong Wang, "Efficient Two-Server Password-Only Authenticated Key Exchange", IEEE Transactions on parallel and distributed systems, vol. 24, no. 9, September 2013