International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 1148–1151

"Review OnDivision and Replication of Data in Cloud for Optimal Performance and Security DROPS"

Afsha Khan Suri,Prof. Nisha Balani,Prof. Amrita Kungwani

Department of CSE,Jhulelal Institute of Technology
Email.Id:-afshasuri10@gmail.com,*nisha.balani@jit.org.in, a.kungwani@jit.org.in*

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 with in the cloud. Therefore,high security measures are required to protect data within the cloud[2]. 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[14]. 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[13]. 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.

Keywords—*Centrality, cloud security, fragmentation, replication, performance*

2. Introduction

Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing[2]. Cloud security issues may stemdue 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 arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.)[11]. 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 of the assets does not solely depend on an individual's security measures. 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 environment that may result in various security concerns[8].

3. Literature Review

Data centers being an architectural and functional block of cloud computing are integral to the Information and Communication Technology (ICT) sector. Cloud computing is rigorously utilized by various domains, such as agriculture, nuclear science, smart grids, healthcare, and search engines for research, data storage, and analysis. A Data Center Network (DCN) [1] constitutes the communicational backbone of a data center, ascertaining the performance boundaries for cloud infrastructure.The DCN needs to be robust to failures and uncertainties to deliver the required

ISSN: 2233-7857 IJFGCN

Quality-of-Service (QoS) level and satisfy service-level agreement (SLA). Here robustness of the state-of-the-art DCNs has been analyzed.

The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models. [2]Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapidtransition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms.

To improve the resource limitation of mobile devices, mobile users may utilize cloud-computational and storage services. Although the utilization of the cloud services improves the processing and storage capacity of mobile devices, the migration of confidential information on untrusted cloud raises security and privacyissues. Considering the security of mobile-cloud-computing subscribers' information, a mechanism to authenticate legitimate mobile users in the cloud environment is sought. Usually, the mobile users are authenticated in the cloud environment through digital credential methods, such as password. Once the users' credential information theft occurs, the adversary can use the hacked information for [3] impersonating the mobile user later on. The alarming situation is that the mobile user is unaware about adversary's malicious activities. In this paper, a light-weight security scheme is proposed for mobile user in cloud environment to protect the mobile user's identity with dynamic credentials.To enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange.The experimental results for the proposed scheme showed significant improvement in turnaround time and energy consumption as compared to the existing scheme.

Quick scattering and access of data in enormous disseminated frameworks, for example, the Internet, has become a standard of our every day life. Be that as it may, undesired long postpones experienced by end-clients, particularly during the pinnacle hours, keep on being a typical issue. [4] Duplicating a portion of the articles at different destinations is one potential arrangement in diminishing system traffic. The choice of what to duplicate where, requires taking care of a limitation improvement issue which is NP-finished all in all. Such issues are known to extend the limit of a Genetic Algorithm (GA) to its limits. Unfortunately, the static GA approach includes high running time and may not be helpfulat the point when perused/compose requests consistently change, just like the case with breaking news.To handle such case we propose a cross breed GA that takes as info the present reproduction conveyance and figures another one utilizing information about the system properties and the progressions happened.There has been an expanding organization of substance dispersion systems [5](CDNs) that offer facilitating administrations to Web content suppliers. CDNs convey a lot of servers dispersed all through the Internet and imitate supplier content over these servers for preferable exhibition and accessibility over concentrated supplier servers. Existing work on CDNs has principally centered around methods for effectively diverting client solicitations to suitable CDN servers to lessen demand inactivity and parity load. Be that as it may, little consideration has been given to the advancement of situation procedures for Web server copies to additionally improve CDN execution. We investigate the issue of Web server imitation situation in detail. We build up a few arrangement calculations that utilization remaining task at hand data, for example, customer dormancy and solicitation rates, to settle on educated position choices. [6] Cloud computing is an emerging paradigm that provides computing resources as a service over a network. Communication resources often become a bottleneck in service provisioning for many cloud applications. Therefore, data replication, which brings data (e.g., databases) closer to data consumers (e.g., cloud applications),

ISSN: 2233-7857 IJFGCN

is seen as a promising solution. It allows minimizing network delays and bandwidth usage. In this paper we study data replication in cloud computing data centers. Unlike other approaches available in the literature, we consider both energy efficiency and bandwidth consumption of the system, in addition to the improved Quality of Service (QoS) as a result of the reduced communication delays. The evaluation results obtained during extensive simulations help to unveil performance and energy efficiency tradeoffs and guide the design of future data replication solutions.

4. Existing System

Cloud computing is characterized by on-demand self-services, ubiquitous network 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.

1] Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing.

2] Cloud security issues may stem 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 arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.)

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. 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.

Performancecan be enhanced by

Developing 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. DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. A controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.

5. Conclusion

DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time can be proposed. The data file can befragmented and the fragments will dispersed over multiple nodes. The can were separated by means of T-coloring. The fragmentation and dispersal will that no significant information was obtainable by an adversary in case of a successful attack. A scheme for outsourced data that takes into account both the security and performance can be introduced.

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 CloudComputing, Vol. 1, No. 1, 2013, pp. 64-77.

ISSN: 2233-7857 IJFGCN

2. D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.

3. 3.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.

4. 4. T. Loukopoulos and I. Ahmad, “Static and adaptive distributed data rep
5. lication using genetic algorithms,” Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp. 1270-1285

6. 5.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

7. 6.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*
8. *Experience*, Vol. 25, No. 12, 2013, pp. 1771-1783.

9. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, “Energy-effificient data replication in cloud computing datacenters,” *In IEEE Globecom Workshops*, 2013, pp. 446-451.

10. Y.Deswarte, L.Blain, and J-C. Fabre,“Intrusion tolerance in distributedcomputing systems,” *In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA*, pp. 110-121, 1991.

11. W. K. Hale, “Frequency assignment: Theory and applications,” *Proceedings of the IEEE*, Vol. 68, No. 12, 1980, pp. 1497-1514.

12. 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.

13. M. Hogan, F. Liu, A.Sokol, and J. Tong, “NIST cloud computing standards roadmap,” NIST Special Publication, July 2011
14. .
15. 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.

16. 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.

17. 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

ISSN: 2233-7857 IJFGCN