International Journal of Research
Available at
https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Division And Replication Of Data In Cloud For Data Security And Increase Performance Using Fragment Placement Algorithm

YEJERLA ANANDKUMAR[1] ,Dr. PATHAN HUSSAIN BASHA[2]

#1Student,Department of CSE, Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India

#2HOD And Assoc Professor, Department of CSE, Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India

ABSTRACT: The issues identified with security and activity defeats by the Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS). In distributed computing, the data is put away on outsider space which brings about a security concerns. The client and lymph organ inside cloud may bargain the information. Along these lines, to ensure information inside the cloud senior secondary school safety efforts are required. Partition an information document into pieces, and repeat the divided information over the cloud lymph organ is done in DROPS methodological investigation. Just a section of a specific information document can be put away by every one of the hub that guarantees that no significant data is uncovered to the attacker even if there should be an occurrence of a fruitful assault.

KEYWORDS: Centrality, Cloud Security, Fragmentation, Replication, Performance.

1.INTRODUCTION

The cloud computing paradigm has reformed the usage and management of the information technology framework. 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 conspicuous candidate for businesses, organizations, and individual users for adoption.However, the benefits of minimum cost, negligible management (from a users perspective), and greater elasticity come with increased security concerns. Security is one of the most crucial aspects among those forbiddingthe wide-spread adoption of cloud computing.Cloud security issues may stem due to the core technologies

implementation (virtual machine (VM) escape, session riding, etc.), cloud service presenting (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.).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 systems security is equal to the security level of the weakest entity. Therefore, in a cloud, the security of the assets does not completely depend on an individual's security measure. The neighboring entities may provide an opportunity to an attacker to detour the user's defenses.

II. LITERATURE SURVEY

Mazhar Ali, Samee U. Khan, DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security IEEE 2015.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[1].

J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, had presented the Cloud computing ontogenesis due to its sum applied science hike the protection yield . So, to achieve the protection as well as performance by using three proficiency , Graphical Word Certification , Fragmentation and Counter , this system provides a better solution. Nowadays, the use of the Graphical Password Assay-mark increases. This is because as compared to alphanumeric method, it is very easy to remember and secure. Fragmentation used to secure data from single distributor point tragedy . In loser situations, Replication can be useful for maintaining availability, reliability and performance. But due to extreme use of bandwidth the extra comeback can also result in high storage cost or drops in systems overall performance. So, here controlled replication is used. The

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

clock time and piece of work on some tone-beginning will get saved in the future work[2]

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. This paper compares and analyzes

10heuristics to solve the fine-grained data replication problem over the Internet. In fine-grained replication, frequently accessed data objects (as opposed to the entire website contents) are replicated onto a set of selected sites so as to minimize the average access time perceived by the end users.[3].

D.Boru, D.Kliazovich, F.Granelli, P.Bouvry,andA.Y.Zomaya, Divided a file into sherd s, and replicate the fragmented information over the cloud nodes. Each of the nodes entrepot only a single fragment of a particular data file. It ensures that even in case of a successful attack, the attacker fail to get meaningful information [4].

T. Loukopoulos and I. Ahmad To improve the resource limit of Mobile devices, mobile users may utilize cloud-computational and storage Service . The processing and storage capacity of mobile devices, the migration of confidential data on untrusted cloud raises security system and privacy government issue get improved by the utilization of the cloud services improves. [5].

K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomayaanalyzed lustiness of the state-of-the-art DCNs. The papers major contribution are: 1) It presented multilayered graph modeling of various DCNs; 2) It studied the classical hardiness Synonyms/Hypernyms (Ordered by Estimated Frequency) of noun metric considering various failure scenario to perform a comparative analysis; leash) It presented the inadequacy of the classical network hardiness metrics to appropriately evaluate the DCN robustness; and 4) It proposed new subroutine to quantify the DCN robustness. Therefore, for the future DCN robustness research , we believe that this work will lay a firm foundation.[6]

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez a very wide sketch had been reviewed which signifies scourge with avail and deployment models of swarm ., this study is presented so as to effectively refine the crude security issues under various areas of swarm in order to comprehend these threats. This study also purpose at revealing different security threats which were under the cloud models as well as network concern to stagnate the threats within cloud, facilitating researcher, cloud supplier and end drug user for noteworthy analysis of threats [7].

K. Lai, M. Feldman, I. Stoica, and J. Chuang, Incentives for cooperation in peer-to-peer networks, in Proc. 1st Workshop Economics Peer-to-Peer Syst., 2003, pp. 631660. In this paper we take a game theoretic approach to the problem of cooperation in peer-to-peer networks. Addressing the challenges imposed by P2P systems, including large

populations, high turnover, asymmetry of interest and zero-cost identities, we propose a family of scalable and robust incentive techniques, based upon the Reciprocative decision function, to support cooperative behavior and improve overall system performance. We find that the adoption of shared history and discriminating server selection techniques can mitigate the challenge of few repeat transactions that arises due to large population size, high turnover and asymmetry of interest[8].

ManishaKalkal, SonaMalhotra, Replication for Improving Availability and Balancing Load in Cloud Data Centres, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015. In this paper, 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 privacy issues. 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 impersonating the mobile user later on. The alarming situation is that the mobile user is unaware about adversarys malicious activities. In this paper, a light-weight security scheme is proposed for mobile user in cloud environment to protect the mobile users identity with dynamic credentials. The proposed scheme offloads the frequently occurring dynamic credential generation operations on a trusted entity to keep minimum processing burden on the mobile device. To enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange[9].

S. M. Khan and K. W. Hamlen, Hatman: Intra-cloud trust management for Hadoop, in Proc. 5th Int. Conf. Cloud Comput., 2012 Hatman extends Hadoop clouds with reputation-based trust management of slave data nodes based on EigenTrust. To obtain high scalability, all trust management computations are formulated as distributed cloud computations. This leverages the considerable computing power of the cloud to improve the data integrity of cloud computations[10].

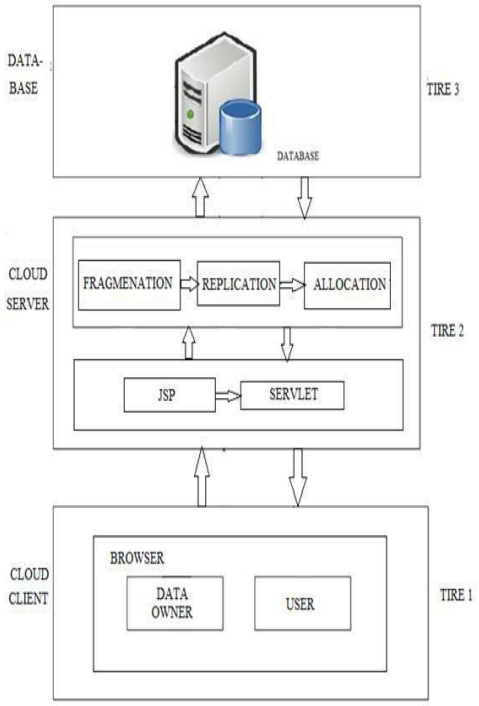
S. Pearson and A. Benameur, Privacy, security and trust issues arising from cloud computing, in Proc. 2nd Int. Conf. Cloud Comput., 2010, pp. 693702. Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organisations and users. In particular, it is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is not compromised. Responsible management of personal data is a central part of creating the trust that underpins adoption of cloudbased services without trust, customers will be reluctant to use cloud-based services[11].

E. Bertino, F. Paci, R. Ferrini, and N. Shang, Privacy-preserving digital identity management for cloud computing, IEEE Data Eng. Bull, vol. 32, no. 1, pp. 2127, Mar. 2009. In this paper we have proposed an approach to the verification of digital identity for cloud platforms. Our approach uses

efficient cryptographic protocols and matching techniques to address heterogeneous naming. We 6 plan to extend this work in several directions. The first direction is to investigate the delegation of identity attributes from clients to CSPs. Delegation would allow a CSP, called the source CSP, to invoke the services of another CSP, called the receiving CSP, by passing to it the identity attributes of the client. However the receiving CSP must be able to verify such identity attributes in case it does not trust the source CSP[12].

III.PROPOSED SYSTEM APPROACH

We propose another thought called DROPS(Division and Replication of Data in Cloud for Optimal Performance and Security) that mutually moves toward the security and execution issues. The proposed DROPS plot guarantees that even on account of a fruitful assault, no significant data is disclosedto the aggressor. We don't rely upon customary cryptographic systems for information security. The non-cryptographic nature of the proposed plan makes it quicker to play out the necessary activities (position and recovery) on the information. We ensure a controlled replication of the document parts, where every one of the sections is repeated once with the end goal of improved security. A distributed storage security conspire mutually manages thesecurity and



execution regarding recovery time.

Advantage:

1) Improve security.
2) Improve performance.
3) No any information is revealed to the attacker.
4) No load on single node of cloud.
5) Numbers of fragments are decided according to owner's choice.

IV.PROPOSED ARCHITECTURE

System Architecture

V.MODULES

1) Cloud Client:-

Cloud client should be Data owner or Data user.

1. Data Owner:-

2. Data owner is responsible for uploading file on cloud as well as view files uploaded by him or others. Data owner has information about the placed fragment and its replicas with their node numbers in cloud.

3. Data User:-

4. Data user is the one who is responsible for downloading files or view files uploaded by others. To download file from cloud he has to be authenticated user otherwise he will be considered as attacker.

2) Cloud Server:-

· Fragmentation:-

This approach is used for fragmenting the file for security purpose at sever side. This approach runs the Fragmentation algorithm. It has file as input and produces the file fragments as output.

 Replication:-

This approach creates replicas (duplicate copy) of fragments. These replicas are useful when one of fragment is corrupted by attacker then to provide file for user admin replaces its replica at that place and combine all fragments and send file to authenticated user or data owner. To make replicas of file fragments this approach runs replication algorithm which takes input as fragments and produces its replicas as output.

 Allocation:-

After the file is spitted and replicas are generated then we have to allocate that fragments at cloud server for storing data. While storing or allocating that fragments we have consider security issues. So we are using T-Coloring Graph concept for placing fragments at different nodes on cloud server. This approach runs Fragment allocation algorithm which takes input as fragments and produces the output as fragments allocated with node numbers.

VI. CONCLUSION

The user has to register in cloud, for each registered user, a unique secret key is generated .the user when wants to upload the file, it gets splits into small chunks and for every upload of file a secret file key is also generated when user wants to download a file, they should enter a secret file key of their file, then splits chunks get merged and can download the file. This provides security at client

level as well as in network level. The aforesaid future work will save the time and resources utilized in downloading, updating, and uploading the file again.

REFERENCES

[1]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.

[2]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.

[3]D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,"Energy-efficient data replication in cloud computing datacenters", In IEEE GlobecomWorkshops,pp. 446-451,2013.

[4]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.

[5]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.

[6]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.

[7]K. Lai, M. Feldman, I. Stoica, and J. Chuang, "Incentives for cooperation in peer-to-peer networks", in Proc. 1st Workshop Economics Peer-to-Peer Syst.,pp. 631660,2003.

[8]ManishaKalkal, SonaMalhotra, "Replication for Improving Availability and Balancing Load in Cloud Data Centres", International Journal of Advanced Research in

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[9]S. M. Khan and K. W. Hamlen, Hatman,"Intra-cloud trust management for Hadoop", in Proc. 5th Int. Conf. Cloud Comput., 2012

[10] S. Pearson and A. Benameur, Privacy, "security and trust issues arising from cloud computing", in Proc. 2nd Int. Conf. Cloud Comput.,pp. 693702,2010.

[11] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving digital identity management for cloud computing", IEEE Data Eng. Bull, vol. 32, no. 1, pp. 2127, Mar. 2009.

[12] F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers bootstrapping and prediction of trust", in Proc. 10th Int. Conf. Web Inf. Syst. Eng., pp. 275289,2009.

[13] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman filter based adaptive maintenance for dependability of composite services", in Proc. 20th Int. Conf. Adv. Inf. Syst. Eng.,pp. 328342,2008.

[14] Y. Wei and M. B. Blake, "Service-oriented computing and cloud computing: Challenges and opportunities", IEEE Internet Comput., vol. 14, no. 6, pp. 7275, Nov./Dec. 2010.

Author's Profile

YEJERLA ANANDKUMAR Completed B.Tech in 2008.at present he is pursuing M.Tech In Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India

Dr. PATHAN HUSSAIN BASHA has his B.Tech (UG) Degree received from Andhra University, M.Tech (PG) Degree received from Acharya Nagarjuna University and Ph.D received from Rayalaseema University Kurnool in the year of 2018. He is dedicated to Teaching Field from the Past 12 Years. He Has Guided 26 P.G

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Students And 40 U.G Students. His Research area is communication networks and Included Artificial Intelligence. At Present He is Working as Associate Professor and HOD in Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India. He Is Highly Passionate And Enthusiastic About her Teaching And Believes That Inspiring Students To Give Of His Best In Order To Discover What He Already Knows Is Better Than Simply Teaching.