ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse187952020.pdf
https://doi.org/10.30534/ijatcse/2020/187952020

User Authenticated and Approved Load Balancing In Cloud Computing

Nune Sreenivas[1] , Gadiparthi Manjunath[2]
[1]Assistant Professsor, School of Electrical and Computer Engineering Addis Ababa Institute of Technology,AAU, ns_maruthi@yahoo.com
[2]Assistant Professsor, School of ITSC,Addis Ababa Institute of Technology,AAU , gmanjunathc2000@gmail.com

ABSTRACT

Load balancing in the cloud computing is an important aspect in this technology, there are many challenges in load balancing in cloud computing. In general space for data in cloud is allocated by the main server. Based on the data load level the data stored in the cloud is been relocated by the main server for balancing needs. In most of cases this relocation of data is been unaware to the data owner. This scenario is identified as a data breach or as a confidential issue for the cloud owners. For this an solution is been identified in this paper, that space allocation for the data and data stored area is made known to the user, based on the user approval the space allocation is done and based authentication space for the data is relocated if it require. This will make to feel the data owner's confidence over the data security in cloud.

Key words : Load balancing , Data owners, Authentication

1. INTRODUCTION

Data transaction is huge in the data today life, each data owners are willing to store their data is safe and secure manner, in other hand data load is keep on increasing in various time intervals, so cloud data based load balancing challenges and security based challenges are arises day by day in different forms, in this paper general load involved security based challenges are taken into consideration and solution is proposed. Our work is divided two category one is data wrapping and data owner approval for load alteration. [1] [2]

Generally load balancing ideologies are initially classified on the state of system and performance, load balancing state issues initialed while allocating the load to the concern storage servers those allocation is considered as static and dynamic load balancing methodologies. In other aspect sender there are some more techniques to classify the load balancing in the form of sender engaged, receiver engaged and symmetrical

a. Static : In static load balancing methodology a protocol is being fixed , in which the system will not consider the situation of the data load ,There are some set of procedures that not able to alter, need of some initial preparations techniques such are based on time, memory and storage capacity of nodes and so on , to approach the process . Even though this process is simple and easy to process this approach lacks to identify the nature of server, which is actually going to be loaded. This is the major issue in this approach, In approach can be taken to consideration while it is dealing with the limited loads that is low in space occupation. This protocol of load balancing can't be considered for the large and expanding distributed systems technologies.

b. Optimal and Sub optimal: In these methodology the load balancing can be done based on the load collection node ,which collects the load at its node ,based on the load level the load balancer will allocate the load in storage server. In another case of sub optimal there is no such concept of load balancer or the load balancer is not able to make optimal decision making other optimal techniques like shortest job first ,two phase opportunistic load balancing is being applied to give directions to load balancer to take decision in load allocation to balance the cloud data load.

c. Dynamic: This mode of load balancing technique allows load balancer to monitor the data load in the cloud. Nature of the load whether it is over loaded or under loaded. In this technique load in a cloud can be altered or shuffled based on the storage capacity in the cloud. Monitoring of data load is monitored continuous over a time interval based on that the changes is made to improve the performance of the storage cloud. Further this technique as two provisions such as distributive and non-distributive. Which further support in load balancing in cloud [3]

d. Distributive and Non Distributive: In distributive load allocation entire nodes communicate information to disseminate and re-disseminate to complete the task effectively, distributive algorithms mostly in cooperative form to execute the task successfully. In other mode of Non distributive format, some of the nodes will be communicating for load balancing. Here, if there is single node failure also lead to loss of information and recovery of information also is impossible. In the case of semi distributed technique some main nodes take part in load balancing as a clusters as a centralized technique.

2. MEASURING LOAD BALANCING IN CLOUD COMPUTING.

There are many parameters can be considered for load balancing performance measure. In that efficient performance is a parameter based on system effectiveness that is validated with overall performance with various existing load balancing methodologies. The overall running time to balance the load and to complete the task given to the load balancer is considered as a parameter called response time as one of the metrics. The work submission within a period of time on a system is referred as throughput parameter ,which is also can included as a parameter to measure the load balancing technique in cloud by handling of heavy load in very limited time interval.Whenever the load increases or the nodes in cloud increases, uniform load balancing must to be made to increase performance of the cloud, so scalability is considered as a one of the parameter to be considered for performance measure in load balancing in cloud. There are chances for break down in cloud while it is handling enormous data at a limited interval of time, so fault tolerance can be considered as a parameter to measure for load balancing ideology. The time taken for data transfer from fully loaded server to unloaded server is termed as migration time. This aspect can be considered measuring cloud performance in load balancing ideology. Usage of data from the cloud and overall cost may be reduced while using higher resources. The usage of reduced energy expenditure as well as carbon release rate in the cloud system are also measured in the parameter as resource use. Variations of VMs can lead to some imbalance in the cloud, it is considered as degree of imbalance parameter in cloud load balancing.[4][5]

Security and Load Balancing in Cloud Computing

Apart from these parameters for cloudload balancing performance measure in cloud computing, load balancing with security considerations can also be considered as factor that is discussed as a challenge and solution is also recommended, for the foretold issue.

Loss of Data while Load balancing: There are chances of data loss while uploading the data from one server to another server. While there is transfer of data from one server to another for the reasoning of balancing, chances of lack of integrity may occur for the cloud data. This is an accidental human error this should be averted by providing proper security to the data content with a proper methodology. This is been proposed as the work in this paper.

Data Breach while load balancing: This may occur while transferring data from one cloud server to another server for load balancing reason, when a server attains its threshold level , unbalancing may occur to restore the normalcy data should be shifted from one cloud server to another.This may occur purposely by humans to make the data let out. Taking this into consideration, security measures should be made to secure the cloud data from all kind of data integrity based issues, which affects the performance of cloud.

Securing Cloud Data through Message Digest and Data Owner Authentication

Two kind of challenges is identified while transferring from one server to another, for these two challenging task, the two kind solution is been proposed. Securing data through wrapping of data of the particular data owner is a novel ideology which is been proposed to ensure the data integrity. In this methodology the entire data of the data user is made a message digest form with the data owner authorization and authentication.

Here a new algorithm named as BLAKE 2 is been introduced for wrapping the cloud data for the data integrity reasons , BLAKE2 possess some inherent features that enables a better wrapping up technique of cloud data while load balancing the cloud.[6] [7]

Features of BLAKE2b

BLAKE2 possess dual set of algorithmic support for providing security in form as BLAKE2b which meant to provide optimization for 64 bit data encryption as well as wraps the data as in the form of message digest up to 64 bytes as well as BLAKE 2s made optimization to other bit formats like 8 as well as 32.

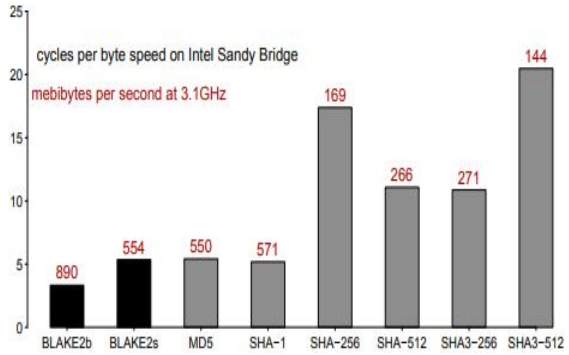


Fig1: A speed comparative study over other hash data wrapping functions that prominent in use.

Less rounds

BLAKE2b provides 10 to 16 rounds for wrapping data for security it is more secure. These rounds of encryption of hashing kind of wrapping of data provides speed of up-to 29% on large inputs, as the wrapping for larger input itself is very less comparing with other algorithms. Similarly very fast wrapping time will be taken while applying this algorithm in lower sized data.

As BLAKE series are good in speed in data wrapping technique, other aspects are also considered for providing a complete compatible security conditions.

Speed based Optimization over number of Rounds

Based on XORs modular functions such as additions and rotations of word BLAKE2B performs word rotations of 64bit with respectively ,here 24 bit rotations is allowed to accomplish two parallel rotations simultaneously with one SIMD instruction set. But the requirement is two similar shifts with a single OR logical operations for the single 25 bits rotations. By this method function cost is reduced, this increases the speed of this function a little .Number of cycles are also been reduced to 16 set of instructions from 18 set of instructions.as a part of 12% reduction in

performance time.[8] [9]

Rotation of 63 –bit is included with an additional aspect as well as logical OR operation with a shift is been followed due to this function a speed of operation is increased a little with shift as well as addition operation is performed in parallel. In addition 63 right rotation as well as single left rotation will increase the performance speed slightly in some form of architectures, where considered as a exceptional cases. This alterations doesn't impact anything in overall platforms functions.

Minimum padding support and completion flag alert

Padding is done in BLAKE2 in final block of data if necessary through null bytes, in the case of data length is the multiples of the block length, padding are not required. This indicates that if the message length as well as the multiples of block length are in similar structure then padding is not required. Length of padding is not considered for calculation as it was done in the previous methods. To improve the further quality of BLAKE 2 performance flags are assigned as a novel method like f_0, and f_1 as support functions as a security functions of padding is transferred to flag that is considered as a finalized flag called as f_0 as ff a set of word in case the processing block is final and then 00 is considered as flag.

In secondary form flag to be finalized one is considered as $f_1$alerts the final node of tree topology based hashing structure to wrap the data that is going to be uploaded and in the server for load balancing .The BLAKE2b's is capable of handling the higher level of 2^{128-1} bytes ought to be enough for handling any set of data wrapping.

Hashing Key for Wrapping Data

Hashing is a form encrypting shield, used for message digest, the same set of key with the support of BLAKE 2s is developed for data wrapping.The arbitrary data is being identifies the padded key , in this technique zeros are padded with the first block of data to generate as a key then first block of data with the succeeding block of the data. Data is totally wrapped with this key as single block. Counter t is considered as the 64 bytes of the block of key apart from length of the key. While wrapping the lossless data compression function is enabled.

Prefix MAC mode is securely used in this model this is the indifferential property in BLAKE2, prefix-MAC is considerably faster than HMAC that highly supports in compression function.[10]

Wrapped Data in Tree Structure

Wrapped data are structured in the form of a tree topology block structure for the clear identification of data. As the tree structure going to extended whenever the data owner includes his data in the structure, the algorithm BLAKE 2s going to support it. The leaf length of the tree normally placed in the powers of 2

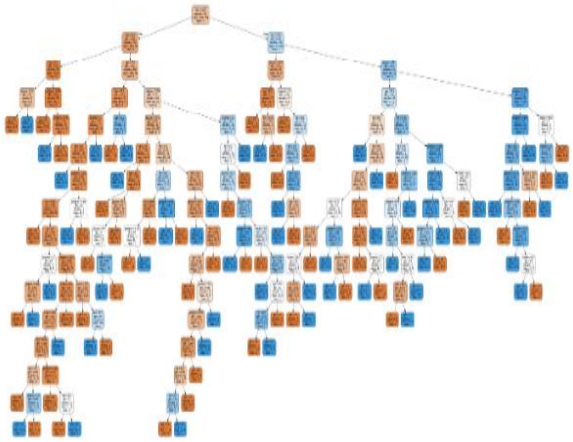


Fig2: BLAKE2s representation of data of various owner

The data are stored in the leaf nodes of the tree as a chunks , each leaf node are wrapped with the BLAKE2s technique in the node offset and node depth parameters develop hash similar function for the data wrap .The finalization flag f_1 indicates start of the particular data node and f_n indicates end of the data node.In this manner the tree structure is made enabled for developing a security wrapping structure for data in the load balancing cloud data.

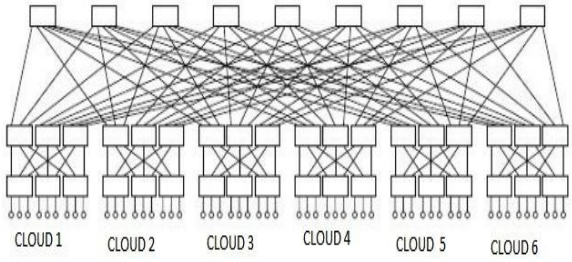


Fig3: Tree structured data arrangement in cloud

Similar to the fig3 the cloud data is wrapped and arranged in the cloud in load balanced form. Load unbalancing may occur while the owner of data increases the load of data in the cloud. In that case to balance the cloud owner will alter the data position without the knowledge of the data owner. This may felt as the data breach by the data owner, to avoid this an authentication based data alteration is recommended through this work, with third party authorization.[11]

3. SAML BASED AUTHORIZATION AND AUTHENTICATION FOR CLOUD DATA SECURITY

Security assertion markup language is the tool to be used for securing data while the cloud owner tends change the position of the data, it makes sign on in format known as single sign-on SAML it enables digital signed documents. As it provides complex single sign on while deploying this technique, in other hand this set up will enable authentication in incomparable level. This mode of security was developed for the secure communication among business and enterprises. As this technique provides the

security in three modes, initially principal, the identity support (IDS) and Authentication Support Provider (ASP)

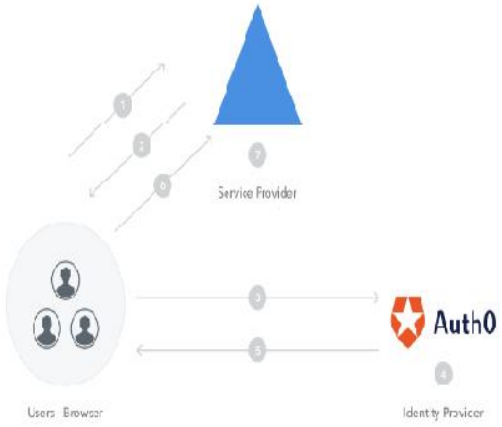


Fig4: SAML authentication process.

SAML Process Steps

i. A common account is created from both cloud space provider and the cloud data provider. Through Auth0, a common authentication and monitoring forum.

ii. Cloud data provider proves his data authentication and with his authentication, he proves authentication with the data load and the space he require in the cloud.

iii. Cloud owner proves his authentication and what space he can allocate for the data owner to store his data.

iv. Based on this information Auth0 generates the report on the cloud area where the data is going to be stored and size of the data.

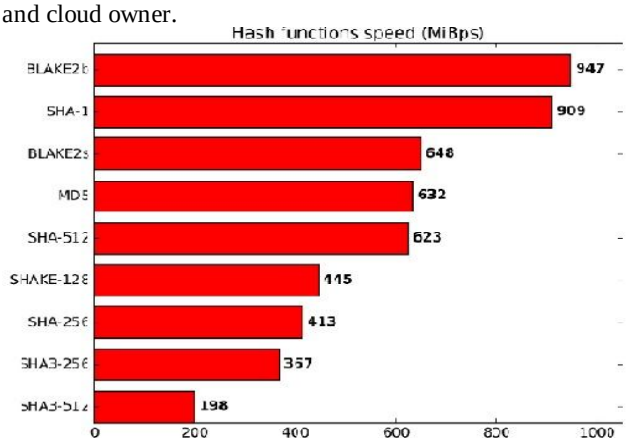
v. Whenever the data owner wants to increase the data level, owner will request Auth0 provide permission to upload the data in stipulated cloud space, this will be reported to the cloud owner, after the permission cloud owner the data will be uploaded.

vi. Whenever the load unbalance occur, the cloud owner will intimate to the data owner to reduce to the data level in the cloud through Auth0, if he cannot reduce the data in cloud , the cloud owner will allocate another space for some commercial to the data owner to store the data.

vii. Changed space address will be intimated to data owner through Auth0 by the cloud owner. After getting approval of the data owner only the alterations will occur. Whenever this alterations occur cloud owner should get approval through the Auth0 ,for this changes

viii. This will occur through key exchange process in SAML authentication technology.

SAML coding provides the communication between cloud owner and cloud user. Through SAML secure communication is established between cloud data owner and cloud owner.



A comparison study was conducted BLAKE with other hashing algorithms for secure wrapping process in that BLAKE was performing well in speed of hashing and as well as providing multilevel security to the data. In our other study analysis SAML is the technology which is running in between cloud data owner and cloud owner, to ensure safe and secure data transaction and movement.[12] [13]

4. CONCLUSION AND FUTURE ENHANCEMENT

The work based on secure load balancing finds the solution for the prolonged security issue called data breaching and data loss. The proposed technology will providing satisfactory security for both cloud data owner and cloud owner. In future enhancement this technique can be extended to multiple level cloud area ,where vulnerability is much higher than the present level.

REFERENCES

1. PAWAN KUMAR and RAKESH KUMAR (2019), “Issues and Challenges of Load Balancing Techniques in Cloud Computing: A Survey”, Vol. 51, No. 6, Article 120.

2. TejashriKhandve, MeghaTalekar, SheetalDhiwar (2015), "Security and Load Balancing In Cloud Computing", Volume 4 Issue 10.
3. Mr. Avinash R. Dhok, Ms. Ashwini P. Kolhe, Ms. Neha V. Lutade, (2015), "A Survey on Scalable Data Security and Load Balancing in Multi Cloud Environment", Volume 1, Issue 8, ISSN (online): 2349-6010.
4. Sandhiya R, D.Radhika., G.Sasikala (2019), "Dependability of the Users in Cloud Environment Using load Balancing and Integrity of Data",) ISSN: 2249 – 8958, Volume-8 Issue-6S.
5. SaurabhDey, Srinivas Sampalli and Qiang Ye (2016), "MDA: message digest-based authentication for mobile cloud computing", Vol 5, issue 8.
6. Osama Harfoushi1 &Ruba Obiedat (2018), "Security in Cloud Computing Using Hash Algorithm: A Neural Cloud Data Security Model", Vol. 12, No. 6, ISSN 1913-1844.
7. M. Vedaraj, M. VigilsonPrem (2017) "A Survey on Data Security in Cloud Computing using Cryptography", Volume 178 – No.4.
8. https://docs.idaptive.com/Content/Applications/AppsScriptRef/SAMLAuthProcess.htm
9. https://auth0.com/blog/how-saml-authentication-works/
10. Chang, S., Perlner, R., Burr, W.E., Turan, M.S., Kelsey, J.M., Paul, S., Bassham,L.E.: Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Compe-tition. NISTIR 7896, National Institute for Standards and Technology (November2012)
11. Duong, T., Rizzo, J.: Flickr's API Signature Forgery Vulnerability. http://netifera.com/research/ (September2009)
12. Neves, S., Aumasson, J.P.: Implementing BLAKE with AVX, AVX2, and XOP.CryptologyePrint Archive, Report 2012/275 (2012) http://eprint.iacr.org/2012/275.
13. Aumasson, J.P., Meier, W., Phan, R.C.W.: The hash function family LAKE. InNyberg, K., ed.: FSE. Volume 5086 of LNCS., Springer (2008) 36-53
14. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: On the indi_erentiability of thesponge construction. In Smart, N.P., ed.: EUROCRYPT. Volume 4965 of LectureNotes in Computer Science. Springer (2008) 181-197
15. Prasadu Peddi (2020), "Public Auditing Mechanism toVerify Data Integrity in Cloud Storage", ISSN 2347 – 3983, Volume 8, No 9, pp: 5220-5225.
16. G. Sekhar Reddy, Dr Ch. Suneetha (2020), "Conceptual Design of Data Warehouse using Hybrid Methodology", ISSN 2278-3091 ,Volume 9, No 3, pp: 2567 – 2573.
17. Nida Kousar G, Dr. Dayanand Lal N (2020), "A Virtual Machine Introspection in Cloud Computing for Intrusion Detection", ISSN 2278-3091 , Volume 9, No 3, pp: 2662– 2666.