DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5501

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A NOVEL TWO-LEVEL MONITORING APPROACH FOR CLOUD RESOURCE ALLOCATION USING VIRTUALIZATION

Ranjith Kumar. T
PG Scholar, Department of Computer Science and Engineering,
Pondicherry Engineering College
Puducherry, India

Dr. Karunakaran. E
Associate Professor, Department of Computer Science and Engineering,
Pondicherry Engineering College
Puducherry, India

Abstract: Cloud Computing has emerged as an advantageous technology from the decade due to its ease of access, cost and complexity being the flexible features. The benefits of the cloud us fulfilled through resource allocation strategies followed for supplying the demands of the growing user requirements. Improper cloud resource handling and naïve user analysis degrade the allocation and resource utilization of the network. This paper proposes a Two-Level monitoring User-Resource monitoring scheme integrated with virtualization so as to improve cloud performance. The ceasing resource allocation and monitoring factors can be evaded through appropriate levels of examination. This prevents inappropriate failures in the network and service declines for the end users.

Keywords: Cloud Computing; Differential Load Function; Level Monitoring; Resource Allocation; Virtualization

I. INTRODUCTION

Cloud computing is one amongst the revolution over a decade. Users have right to access data and works on significant servers while not their own hardware setup. It merely desires a web affiliation. Of these services area unit accessible and classified as 3 ways:

i) Platform as a Service (PaaS)
ii)Infrastructure as a Service (IaaS)
iii)Software as a Service (SaaS)

Client will store the knowledge as he stores like in their own disc drive however to confirm security, many protocols area unit used. Consumer will challenge the files with completely different tokens while not memory of all keys. He encompasses a single personal key and at the time of work cloud generates a key dynamically. The mix of each this personal and public key solely will access the file resources .here we tend to area unit considering a block less information. Cloud storage system stores user information with different secret writing mechanisms. To confirm information integrity we offer auditing on cloud storage systems for applied math data and integrity check. Auditing protocols area unit accustomed verify the privacy protection on consumer information. Third party Auditors area unit audit [1] on behalf of the consumer and verify the integrity of dynamic information hold on within the consumer. Verification is completed for block modification, insertion and deletion supported homomorphic tokens [2] [3].

Virtualization aids IT [4] users and organizations to further optimize their performance of application in a cost-effective and flexible manner. Recent virtualization concentrates over virtual server that is intended to meet the security requirements of the end-users. Virtualization requires virtual machines with operating system and Virtual Machine Monitor (VMM) to acquire its service.

Apart from security, unit reliability-related problems in virtualization have an effect on performance of cloud. For example, the supplier could mix too several Virtual Machines onto a physical server. This may end in performance issues caused by impact factors like limited CPU cycles or I/O bottlenecks. These issues will occur during a ancient physical server, however they're a lot of seemingly to occur during a virtualized server as a result of the association of a single physical server to multiple Virtual Machines such they all contend for important resources. Thereby, management tasks like performance management and capability planning management area unit a lot of important during a virtualized environment than during a similar physical surroundings. This means that IT organizations should be ready to incessantly monitor the employment of each physical servers and Virtual Machines in real time. This capability permits IT organizations to avoid each over- and underutilization of server resources like CPU and memory and to allot and reapportion resources supported dynamic business requirements. This capability additionally allows IT organizations to implement policy-based remedy that helps the organization to make sure that service levels area unit being met [2] [7]

Resource over commitment [5][10] is a technique that has been recognized as a potential answer for addressing the above- mentioned wastage problems. It primarily consists of allocating Virtual Machine (VM) resources to PMs in excess of their actual capacities, expecting that these actual capacities won't be exceeded since VMs are not possible to utilize their reserved resources totally. Therefore, it has nice potential for saving energy in cloud centers, as VMs will currently be hosted on fewer ON user devices. Resource over commitment could, however, lead to Processing Machine (PM) [9] over-loading, that happens once the mixture of requested resources of the VMs regular on some PM will exceed the PM's capacity, probably ensuing in the degradation of the performance of some or all of the VMs running on the overloaded user devices.

According to [6] remote information possession checking that permits unlimited range of file verification integrity having most time is predicated on the storage of the cloud user. The authors in [6] intended to target cloud consumer to renew the key on every occasion once it challenges the cloud for an equivalent file in the meantime to access the file it wants timestamp key to transfer the file. This timestamp secret is modified in keeping with this time and date. These keys area unit firmly send to the cloud user's mail to confirm high security. The aim of this approach is that the file will challenge with completely different keys. If any unauthorized person will notice the personal key it's unfeasible to induce a public key even it hacks by the unauthorized person then he wants the timestamp key. This approach is safer and it wants a straightforward challenge tokens to the cloud server. Just in case of auditing, Tamper Proof Authentication (TPA) audits the files on cloud servers, therefore we tend to maintain the one secure key to verify the info integrity by the TPAs. in keeping with k-anonymity of knowledge privacy, even the auditor isn't ready to read the particular information he will ready to see solely the applied mathematics data and also the total server usage. Information is going to be in encrypted format he will challenge solely the encrypted blocks. During this technique the keys were generated to the consumer secure mail. If the general public keys area unit exposed to the cloud that not solely is ample to access as a result of it conjointly wants the personal key.

VM migration [8] [11], wherever a number of the VMs hosted by the overloaded user device to alternative under-utilized or idle user devices, has been adopted as a answer for handling user device overloading.

II. PROBLEM DEFINITION

Dedicated resource and user monitoring agents' deficiency in cloud system minimize the performance of resource allocation and stabilization over a vast user system. Integrating the virtualization with a scalable monitoring and assessing monitoring units, a novel proposed approach is given in this manuscript. The proposed approach intends to improve network performance with respect to resource allocation and user behavior modeling. The modeling approach is based on the consistency and communication initiated by the user so as to improve the quality of optimization.

III. PROPOSED APPROACH

Considering the fact that encrypting data from the user end is not mandatory, we assimilate the functions of security and reliability monitoring units (SM and RM) to the cloud access resource. The function of a security monitoring unit is to distinguish between trusted VM and adversaries. SM monitors the behavior of the VM it is associated it through direct and indirect trust factors. SM does not recommend VM utilization rather it scrutinizes the behavior of the VM to pursue its service. SM notifies the hypervisor to determine the service levels of the VM that is intensive under level 2 scrutinizing.

The process of our proposed approach with its components is described as in Figure 1.

A. Secure Monitoring (SM) Unit

The virtual machine incorporates SM to administer security. SM acts as a controller and scrutinizing agent to identify and mitigate adversary effects with lesser complexity. In order to prevent resource exhaustion due to intensive VM monitoring, SM relays information of the VM that are requested by the hypervisors. To protect user resources, two-level monitoring is initiated by the SM. The two-level monitoring overrules when monitoring is more vital; with identical events over different time intervals. SM possesses two-levels of monitoring that are briefed as follows:

i. Resource level and
ii. User level

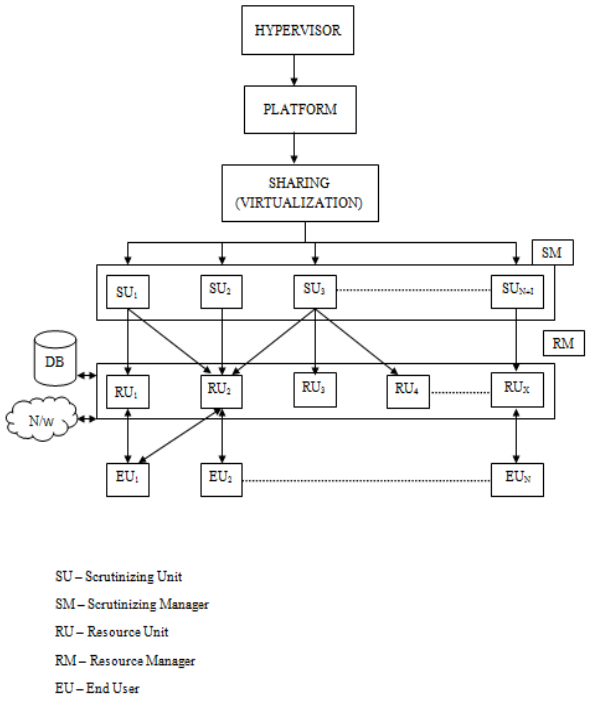

Figure 1 Architecture of the proposed Approach

i. Resource level monitoring

In this level monitoring SM ensures tamper-free nature of the allocated resources. SM verifies if any false data or irrelevant/ compromising-kind of data is being injected to the resource after utilization. If the resource is found to be tampered then SM instructs the resource manager to liberate the resource such that a new resource is further allocated by the resource manager. Resource level monitoring improve efficient management and optimization at the time of allocation and reallocation.

ii. User Level Monitoring

SM monitors the behavior of the user at the time of communication. Monitoring is initiated once the communication request of the user is processed. Overruling/ false credentials sharing are the basic behavior of the users that are monitored by the SM. If the user is found to be vulnerable, the communication session is terminated from the resource manager as directed by the SM. The resource is freed and queued for further allocation.

B. Reliable Monitoring Unit (RMU)

The reliable monitoring unit ensures the feasibility of communication, response, processing and sharing at more optimized manner. The RM interacts with the VM so as to allocate resources to the requesting users. The user requests are forwarded to the resource manager through dedicated spooling services. RM ensures the availability of the virtual machine for further allocation. The virtual machine and RM controls over user input, load balancer and resource managing center.

User Input: User input concerns the available users and their traffic requests. User's traffic request is subjected to change over time and desired resource that is to be shared.

Load Balancer: Load balancers map user request with the corresponding services pre-fetching the knowledge of the resource centers. A dedicated load balancing component ensures virtual machine state; either idle or busy. If the virtual machine is idle, this component ensures the proper assignment of the idle virtual machines and their current state of resource management.

Resource management center: Resource management center directly interacts with the resource manager and other services so as perform integrated assignment of resource allocation and sharing.

RM employs a differential algorithm to improve response of the users based on time factor and this in turn improves monitoring precision

Step 1: Differential balancer maintains a state table for virtual machines and state of VM's (busy/idle), at the starting all VM's are assigned to "0".
Step 2: The resource center controller receives the new request.
Step 3: The Differential balancer receives a request from the resource center controller for further allocation.
Step 4: Differential balancer checks state table from the beginning unless first VM is found available, 1.
This controller receives the VM's id from Differential Load balancer.
The Differential balancer sends request to VM identified by that id.
Differential balancer updates the hash table. If not Found, 1 is returned by the Differential balancer.
Step 5: When VM completes its request processing, controller provides service replies to the users.
Step 6: If the queue is full with the requests, then the controller checks for it and, if any continue from step 3.
Step 7: Continue from step 2.

IV. EVALUATION

The evaluation of the proposed two-level monitoring is carried out by implementing the concept using JAVA as the front-end and MYSQL as the back-end. For further support, we utilized Drive HQ for resource sharing and allocation in a global manner. The complete process is integrated using Netbeans IDE in windows platform.

Virtual Machine Load

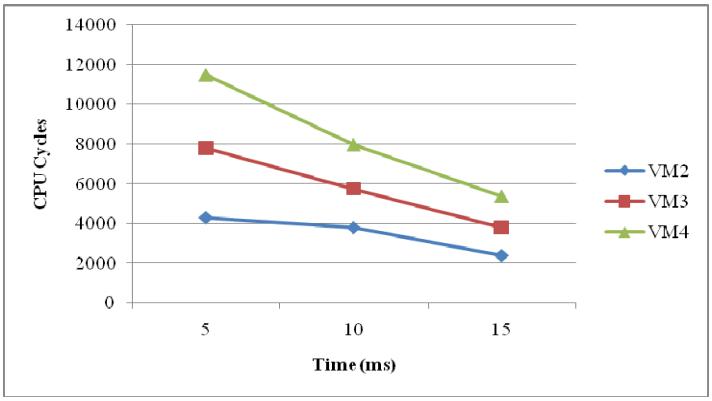

Figure 2 VM Load

The load handled by each of the virtual machine with respect to time quantum is illustrated in Figure 2. The load of the VMs is handled, allocated and reassigned by the resource center component optimized by the RM.

Throughput

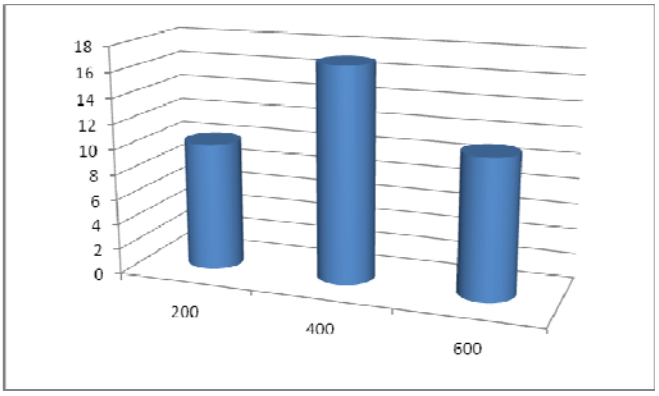

Figure 3 Throughput

Throughput refers to the expected ratio of output observed over an average execution time. The execution time is computed over a series of tasks. The graph in Figure 3 shows the throughput ratio of each task.

V. CONCLUSION

This manuscript proposes a Two-level cloud monitoring approach to retain network performance through intensive monitoring. Monitoring is categorized as user level and resource level to improve optimal network and resource sharing throughout. The number of users is parallel served with lesser imbalance in request mapping; the RM and load balancing component serves the process of efficient resource allocation. The SM prevents unnecessary interruption of adversaries through intensive resource and user monitoring. The integrated approach improves cloud service performance over distributed user system using virtualization. The performance of the proposed two-level monitoring approach is verified by measuring the VM load throughput.

VI. REFERENCES

[1] Y. Zhu, H. Hu, G. J. Ahn and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[2] H. Liu, C. Xu, H. Jin, J. Gong, and X. Liao, "Performance and energy modeling for live migration of virtual machines," in international symposium on High performance distributed computing , 2011.

[3] J. Yu, K. Ren, C. Wang and V. Varadharajan, "Enabling Cloud Storage Auditing With Key-Exposure Resistance," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167-1179, June 2015.

[4] G. Rowel, "Virtualization: The next generation of application delivery challenges," 2009.

[5] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Towards energy-efficient cloud computing: Prediction, consolidation, and overcommitment," IEEE Network Magazine, 2015.

[6] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[7] F. Sabahi, "Security of Virtualization Level in Cloud Computing," in Proc. 4th Intl. Conf. on Computer Science and Information Technology, Chengdu, China, 2011, pp. 197-201.

[8] H. Liu, C. Xu, H. Jin, J. Gong, and X. Liao, "Performance and energy modeling for live migration of virtual machines," in international symposium on High performance distributed computing , 2011.

[9] J. Espadas, A. Molina, G. Jiménez, M. Molina, R. Ramírez, and D. Concha, "A tenant-based resource allocation model for scaling software-as-a-service applications over cloud computing infrastructures," Future Generation Computer Systems, vol. 29, no. 1, pp. 273-286, 2013.

[10] Mohamed Abu Sharkh, Manar Jammal, Abdallah Shami, and Abdelkader Ouda, 2013 "Resource allocation in a networkbased cloud computing environment: design challenges". Communications Magazine, IEEE, 51.11, 46-52, IEEE.

[11] Z. Xiao, W. Song, Q. Chen, "Dynamic resource allocation using virtual machines for cloud computing environment", *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1107-1117, Jun. 2013