ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

A Enhancing Resource Utilization Using QoS Based Load Balancing Algorithm Cloud Computing

Savita Devi[1], Rachna Gupta [2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & NGF College of Engineering &Technology
Palwal, Haryana, India

Abstract

Cloud computing is the expansion of distributed computing, parallel computing and grid computing. It offers quick, secure, comfortable data storage and net computing facilities over the internet. The facilities are provided to subscriber in pay per-use-on-demand model. The primary objective of utilizing resources from cloud is to decrease the cost and to enhance the performance with respect to request response time. Hence, optimizing the resource uses through effective load balancing mechanism is necessary. The primary objective of this paper is to establish and carry out an Optimized Load balancing algorithm in IaaS virtual cloud environment that objectives to use the virtual cloud resources effectively. It reduces the applications cost by efficiently utilizing cloud resources and finds the virtual cloud resources that must be proper for all the applications. The web application is produced with several modules. These modules are taken as tasks and these tasks are presented to the load balancing server. The server which includes our load balancing schemes redirect the tasks to the representing virtual machines made by KVM virtual machine manager according to the load balancing algorithm. If the database size inside the machine is greater than the load balancing algorithm utilizes the other virtual machines for advanced incoming request. The load balancing mechanism are measured for several QoS performance metrics i.e. average execution times, cost, CPU usage, throughput, memory usage, disk space, network transmission and reception rate, scheduling success rate and resource utilization rate for the no. of virtual machines and it enhances the scalability among resources utilizing load balancing mechanisms.

Keywords:
Cloud Computing, Load Balancing, Infrastructure as a Service (IaaS), Round Robin Scheduling, Assignment Approach, KVM

I. INTRODUCTION

Cloud computing [1]-[3] is the usage of computing resources (software and hardware) that are provided as a service through a network (generally the Internet). Cloud computing trust remote facilities with a subscriber's data, computation and software.

Subscribers access cloud-based applications by a light-weight desktop or a web browser or mobile application whereas the business software and subscribers data are saved on servers at a remote place. Cloud computing permits enterprises to get their applications up and working faster, with enhanced maintainability and less management, and enables IT to more quickly adjust resources to fulfill fluctuating and irregular business needs. As computers became more dominant, technologists and scientists disclosed ways to build large-scale computing power present to more subscribers by time sharing, experimenting with algorithms to offer the optimal usage of the platform, infrastructure and applications with prioritized access to the CPU and efficiency for the end subscribers.

In cloud computing, load balancing [4], [5] is another significant technology which comes inside the cloud computing platform. As the no. of subscriber increases for the cloud resources the cloud resources should have the ability to facilitating to the 'n' no. of subscribers request. For the better accessibility of cloud resources and for the shorter response time for the subscriber request, load balancing plays a primary part in IaaS virtual cloud computing environment.

II. DATA SECURITY IN CLOUD

The enterprises move to cloud and obtain the space for data buffering. This data buffering is certainly less expensive for them if compared to the in-house data buffering but the question is, if this data buffering in cloud is also protected and advantageous for enterprises. Thus, one of the most approaching tasks for enterprises is the data storage security. To understand the security problem in Cloud Computing, it is significant to know the Cloud Computing architecture. Once you know the Cloud Computing architecture then it becomes simpler to understand the data privacy and security problems and also to

solve them. Mostly security problems which raise in Cloud Computing are the result of subscribers/enterprises control lacking on the physical infrastructure. Mostly enterprises don't know where their data is physically buffered and which security techniques are in used to secure data such as whether the data is encrypted or not and if yes, which encryption technique is employed also if the link utilized for data to propagate in the cloud is encrypted and how the encryption keys are maintained (Window Security, 2010). Jensen et al. (2009) showed the technical security problems in Cloud Computing. Since, these problems are more associated with the issues of web browser and web services and not of Cloud Computing. These problems are still very significant to Cloud Computing as Cloud Computing builds a lot of usage of web services and subscribers depend on web browsers to access the facilities provided by the cloud. The most general attacks on web services involve the XML Signature Element Wrapping, where XML signature is utilized for authentication.

Browser Security is also a significant problem in Cloud Computing as in a cloud mostly computation is performed on remote servers and the client PC is only utilized for I/O, and commands authorization to cloud. Thus, standard web browser was a requirement of situation to forward I/O and this was used by different names: web 2.0, web applications or Software as Services (SaaS). Since, the ex of web browser arise the security questions. TLS (Transport Layer Security) is significant in this matter as it is utilized for data encryption and host authentication. XML encryption or XML signature cannot be utilized by browser directly as data can be only encrypted through signatures and TLS are only utilized with the TLS handshake. Thus, browser only supports as a passive data store as mentioned above, understanding the dependencies and relationships among Cloud Computing models is serious for understanding the security issues of it. For all the cloud facilities IaaS is the foundation and PaaS is made on it, while SaaS is made on PaaS and IaaS as explained in the cloud reference model diagram

III. SECURITY BENEFITS OF CLOUD COMPUTING

I have discussed about the data storage problems in Cloud Computing since; one must also view into the advantages of data buffering in Cloud Computing. Craig Balding in his blog 'Assessing the Security advantages of Cloud Computing" discusses about these advantages. He addresses that there are some technical security statements in favor of Cloud Computing considering that we can discover the ways to handle the risks. European Network and Information Security Agency (ENISA) have also investigated on the advantages for enterprises using Cloud Computing. Cloud Computing has a lot of potential to enhance security for enterprises and the ways it can enhance security explained below.

Benefits of Scale: It is a fact that all kinds of security measures which are enforced on a larger scale are less expensive. Thus by using Cloud Computing enterprises obtains better security with same amount of money. The security involves all types of defensive measures i.e. patch management, filtering, human resources and their management and vetting, hardening of virtual machine instances, hardware and software redundancy, strong authentication, effective role-based access control and federated identity management solutions by default, which also enhances the network impacts of collaboration among several partners included in defense . Along with these advantages, other advantages involve:

Multiple Locations: The cloud suppliers by default have economic resources to repeat content and this increment the redundancy and independence from failure. Thus, it offers the disaster recovery.

Edge Networks: Cloud Computing offers quality, reliability increase and less local network issues for enterprises by having processing, storage and delivery nearer to the network edge.

Improved Timelines of Response (incidents): Cloud suppliers have larger to incidents or well-run-larger-scale systems. These systems support in enhanced timelines of response such as due to the early detection of new malware deployment, it can formulate more efficient and effective incident response.

Threat Management: The small enterprises don't have resources to hire specialists for handling particular security problems but cloud suppliers can do that and offer better threat management.

Security as Market Differentiator: For mostly enterprises security is the most significant problem while moving to Cloud Computing. They make selections based on reputation of confidentiality, Cloud Computing advantages, risks and suggestions for information security resilience, integrity and security services provided by supplier. This drives Cloud Computing suppliers to enhance the security to compete in the market.

Standard Interfaces for Managed Security Services: Standardized open interfaces to managed security services (MSS) suppliers are usually offered by the large cloud suppliers. This provides more open market for security services where users can select or

switch suppliers more easily with lesser setup costs. Thus, the more resources can be scaled in a granular manner without considering the system resources, the cheaper it gets to respond to sudden increments in requirement.

Rapid, Smart Scaling of Resources: There are already several cloud resources involving CPU time, storage, web service requests, memory and virtual machine instances which can be frequently scaled on requirement and as the technology is enhancing granular control over resource consumption is increasing. The cloud supplier also have the resources and the rights to dynamically reassign resources for traffic shaping, filtering, encryption etc, when an attack (e.g. DoS) is likely or occurs, to increase support for defensive measures. Thus, cloud suppliers can restrict the impact that some attacks have on the resources availability that legitimately hosted services utilized by the integrated use of dynamic resource assignment and suitable resource optimization techniques.

IV. LITERATURE REVIEW

Nisha Peter et. al. [1]; Here, In this paper authors represent an Small computing works that locally processed and responses to the end users without the use of cloud. For the performance evaluation author had taken IOX platforms as a simulation tool. After the simulation result authors conclude that fog computing is entering an exciting time, where it can positively affect operational costs and it resolves problems related to congestion and latency. Fog computing also provides an intelligent platform to manage the distributed and real-time nature of emerging IoT infrastructures.

KC Gouda et. al.[2]; In this paper authors represent approach needs to be evaluate in different cloud platform for finding the cost effectiveness by using the virtualization. For this author use hypervisor and virtual platform simulation. After the simulation result authors conclude that the complexity and cost of owning and operating computer and network can be significantly reduced.

Ivan Stojmenovic et. al. [3]; In this paper authors investigate Fog computing advantages for services in several domains, such as Smart Grid, wireless sensor networks, Internet of Things (IoT) and software defind networks (SDNs). And examine the state- of-the-art and disclose some general issues in Fog computing including security, privacy, trust, and service migration among Fog devices and between Fog and Cloud. In this paper author applying six motivation scenarios for security and privacy issues every scenarios define different role. After the simulation result authors found that there was some innovations in compute and storage may be inspired in the future to handle data intensive services based on the interplay between Fog and Cloud.

Swati Agarwal et. al. [4]; Here Authors, proposed an efficient architecture and algorithm for resources provisioning in fog computing environment by using virtualization technique. For the performance evaluation author had taken Cloud Analyst as a simulation tool. In this paper author talking about intermediate layer of fog to make the architecture more efficient for better service in terms of network bandwidth, power consumption and response time as well as it reduces the traffic over the internet. After the simulation result authors conclude that the proposed strategy can be allocated resources in optimized way and better than existing algorithms in terms of overall response time, data transfer cost and bandwidth utilization in fog computing environment.

Clinton Dsouza et.al.[5]; In this paper authors proposes a policy-based management of resources in fog computing, expanding the current fog computing platform to support secure collaboration and interoperability between different user-requested resources in fog computing. For this author adopt extensible Access Control Mark-up Language (XACML). In this paper author comprises three core components for fog computing architecture and smart transportation system as an exemplary use-case. In this architecture fog node and fog instance communicate with physical devices and cloud computing data centre in parallel. For Policy-Driven Security Management define different module. After the simulation result author outline key characteristics of fog computing and identify challenges in policy management that are critical for supporting secure sharing, collaboration and data reuse in a heterogeneous environment.

V. PROBLEM DEFENITION

In Cloud Computing engineering, there have been some challenges assuming the management of the load (i.e. memory capacity, CPU load and delay or network load) among the cloud computing resources. The organization case that controls a local cluster maintained by virtual machine technology to provide its subscriber with resource needed by their application is taken. The cloud computing environment is deployed by creating the virtual resource of a machine and sharing the virtual resource according to the user specification. If the no. of subscriber to the specific virtual machine greater than the load balancing server will redirect the new

incoming subscribers request to the other virtual machines in node controller. But, this is general technique which does not focus on throughput, time and efficiency. Meantime the random arrival of load in this environment can lead some server to be highly loaded while other server is not active or only less loaded. Equally load distributing enhances the performance by transferring load from highly loaded server. So we require a growing need to balance the several workflows in cloud environment.

VI. LOAD BALANCING

Load balancing [7]-[9] is a computer networking technique to disseminate workload throughout several computers or network links, a computer cluster, disk drives, central processing units or other resources to obtain optimal resource utilization, minimize response time, maximize throughput and ignore overhead. Utilizing several workflows with load balancing, rather than a single workflow may reduce efficiency of the system by scalability. The load balancing service is normally offered by devoted hardware or software, i.e. a system server or a multilayer switch.

In this research paper we have introduced the some of the load balancing mechanisms which targets the effective usage of the cloud computing resources [10]. First one is the normal load balancing algorithm in which if more no. of subscribers or requests (for example, n = 50) to the specific virtual machine greater than the load balancing server redirect the incoming request to the other virtual machine. The other kind of load balancing algorithm is the load balance depending on the existing disk space or memory space on the virtual machine. Most cloud subscribers utilize the cloud resources either to save or fetch data for some calculation.

Load Balancing Operational Workflow

The assignment procedure is a mathematical programming mechanism which is utilized to detect the optimal solution for requested problems. Fig. 1 illustrates the operational workflow for introduced mechanism.

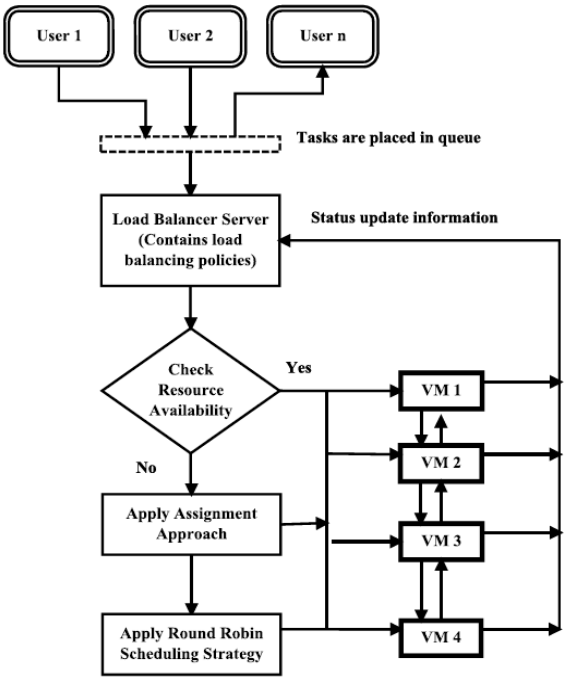

Figure 1: Load Balancing Operational Workflow

The above diagram describes the complete workflow or operation of this paper. For this research paper we have made a web application in which 'n' no. of subscribers is permitted to access the virtual machines effectively from the client side. First the different subscribers utilize the application and send the task to the server. The subscribers requests are positioned in the task queue and it is forwarded to the load balancer. The load balancer examines for the existed virtual resources which are linked to it and it also has the status information of each virtual machine which is linked to it. The status information shows the status of each virtual machine i.e. whether it is in busy state or in presented state. Depending on the virtual machines status the task can be assigned to the virtual resources. If no. of tasks is existed to no. of existed virtual resources the tasks are loaded to the suitable virtual machine according to the cost matrix table. If the no. of incoming tasks is not equal to the no. of existed virtual resources then we employ the assignment mechanism algorithm to detect the virtual machine for the requested application and implement the round robin technique to perform the tasks which are available in the queue depending on mentioned time slots of the respective virtual machines.

VII. EXPERIMENTAL RESULTS

Experimental Setup: The Ubuntu operating system is established to provide support to the resources virtualization utilizing the hypervisors i.e. KVM

which offers the KVM virtualization for making the virtual machines. The needed OS is established in the virtual machines and MongoDB database for the application also loaded in the virtual machines. The server side program is loaded into Ubuntu OS which behave as a server and also behave as a load balancer.

Resource CPU Usage: The Fig.2 shows the CPU usage performance of VM1, VM2 & VM3. In this graph the first virtual machine VM1 is computed by the application and then the VM2 and the VM3 respectively. At starting the VM1 has 20% of CPU utilization. After some time the CPU utilization of VM1 is enhanced to 55% at that time the novel VM is detected (VM2) and novel incoming requests are sent to VM2. At specific time the VM2 load also satisfies the threshold value of 50% and again novel VM is detected (VM3) and further incoming request are sent to VM3. By this introduced procedure the various virtual machines are equally balanced at some point and inactive virtual cloud resources are utilized effectively.

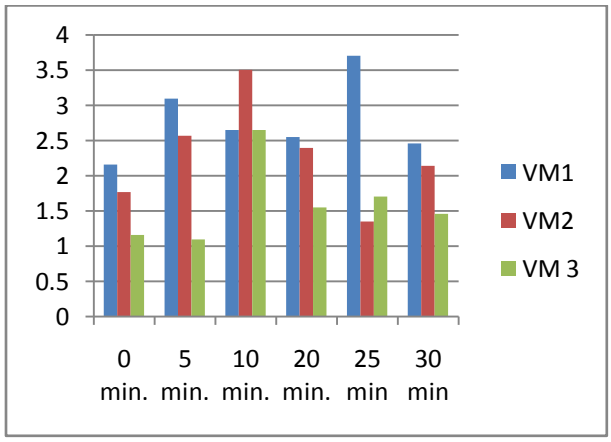

Figure 2: CPU Usage

Resource Memory Usage: The Fig. 3 shows the memory utilization between different virtual machines (VM1, VM2 & VM3). At starting each virtual machine has suitable memory performance. Then the first virtual machine is get computed and if the first virtual machine performance decreases or if it obtains the threshold value then the load balancer indicate the other virtual machine request which has high memory space.

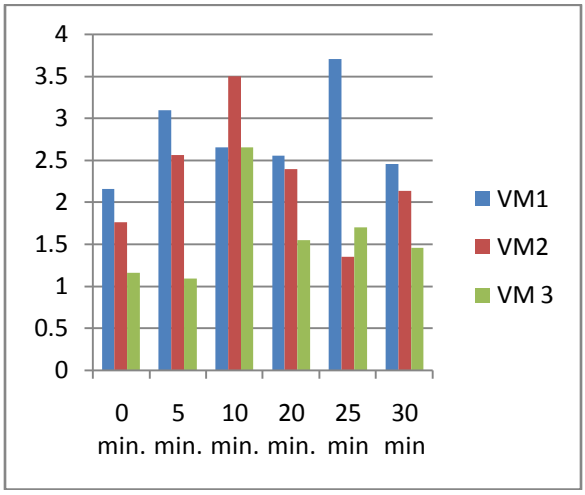

Figure 3: Memory Usage

Average Execution Time: The execution time (in sec) of every task on corresponding virtual machines is considered and those values are defined in the cost matrix table. Mean execution time value is computed utilizing the Eq.(1). Fig. 4 illustrates the mean execution time of tasks on every cloud resources. So from the graph, the mean execution time of tasks in VM2 is lower than the execution time of tasks in VM1. Because tasks are operating in VM2 efficiently uses the cloud resource as compared to VM. And also both the virtual resources are presented with different configurations within the node controller.

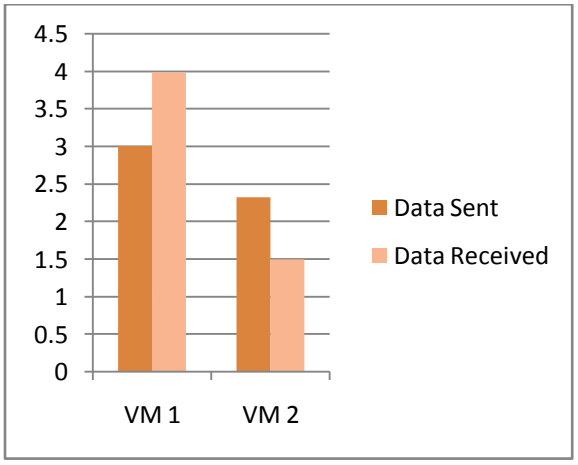

Figure 4: Average Execution Time of Tasks

Throughput: The virtual resources throughput on various tasks are computed by the product of no. of tasks and mean execution time of every task utilizing the Eq.(2). Fig.5 illustrates the throughput value of virtual cloud resources. Depending on the mean

execution time computation, in comparison of VM1, VM2 increases the throughput value.

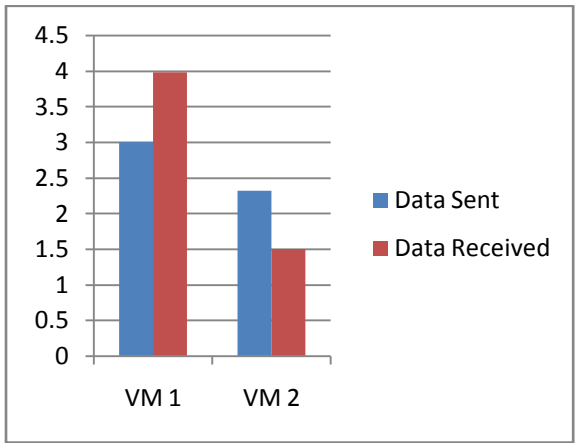

Fig.5. Throughput of virtual resource

VII. CONCLUSION

In this paper we talked about QoS based load balancing procedure for several workflows in IaaS cloud environment. We have taken load balancing situations for independent tasks. Some load balancing mechanisms depend only on the memory and CPU utilization and not focused at tasks execution time. So we have introduced the assignment mechanism depending on cost matrix table which balance the load by sending the task to the allocated virtual machines. This procedure depends on the tasks execution time on every virtual machine. At last the CPU, memory utilization, mean execution of tasks, throughout time, resource usage rate and scheduling success rate of every virtual machines are maintained depending on load balancing situations. This work depends on load balancing between the independent tasks on virtual cloud environment and the future work assumes all the dependent tasks in IaaS cloud environment.

REFERENCE

[1] Nisha Peter, "Fog Computing and Real time Application", International Journal of Emerging Technology and Advanced Engineering, Vol. 5, Issue 6, pp 266-269, June 2015.

[2] Kc gounda, Anurag Patro, Dines Dwivedi and Nagaraj Bhat "Virtualization approaches in cloud computing" International Journal of Computer Trends and Technology (IJCTT), Vol. 12, Issue 4, pp161-166, June 2014.

[3] Ivan Stojmenovic and Sheng Wen," The Fog Computing Paradigm: Scenarios and Security Issues", In the Proceedings of Federated Conference on Computer Science and Information Systems, Vol. 2, pp. 1–8, 2014.

[4] Swati Agarwal, Shashank Yadav and Arun Kumar Yadav," An Efficient Architecture and Algorithm for Resource Provisioning in Fog Computing", I.J. Information Engineering and Electronic Business, pp 48-61, January 2016

[5] Clinton Dsouza, Gail-Joon Ahn and Marthony Taguinod," Policy-Driven Security Management for Fog Computing: Preliminary Framework and A Case Study", IEEE IRI 2014, No. 13, pp 16-23, August 2014.

[6] K.P.Saharan and Anuj Kumar," Fog in Comparison to Cloud: A Survey", International Journal of Computer Applications (0975 – 8887), Volume 122 – No.3, pp 10-12, July 2015.

[7] T.Rajesh Kanna, M. Nagaraju and Ch.Vijay Bhaskar," Secure Fog Computing: Providing Data Security", International Journal of Research in Computer and Communication Technology, Vol 4, Issue 1, pp 53-55, January– 2015.

[8] D.C.Saste, P.V.Madhwai, N.B.Lokhande and V.N.Chothe," FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology", International Journal Computer Technology and Application, Vol 5(5), pp 1768-1771, Sept.-Oct. 2014.

[9] Tom H. Luan, Longxiang Gao, Zhi Liz, Yang Xiang, Guiyi Wey, and Limin Sunz," Fog Computing: Focusing on Mobile Users at the Edge", arXiv:1502.01815v3 [cs.NI] , pp 1-11, 30 Mar 2016.

[10] Rajesh Bose, Murari Krishna Saha and Debabrata Sarddar," Fog Computing Made Easy with the Help of Citrix and Billboard Manager", International Journal of Computer Applications (0975 – 8887), Volume 121 – No.7, pp 19-23, July 2015.

[11] Viraj G. Mandlekar, VireshKumar Mahale, Sanket S.Sancheti and Maaz S. Rais," Survey on Fog Computing Mitigating Data Theft Attacks in Cloud", International Journal of Innovative Research in Computer Science & Technology, ISSN: 2347-5552, Volume-2, Issue-6, pp 13-16, November 2014.

[12] Durairaj. M and Kannan.P," A Study On Virtualization Techniques And Challenges In Cloud Computing", International Journal of Scientific & Technology Research, ISSN 2277-8616 , Volume 3, Issue 11, pp 147-151, November 2014

[13] Kamyab Khajehei," Role of virtualization in cloud computing", International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Volume 2, Issue 4, pp 15-23, April 2014.

[14] Thogaricheti Ashwini and Mrs. Anuradha.S.G," Fog Computing to protect real and sensitivity information in Cloud", International Journal of Electronics and Computer Science Engineering, ISSN- 2277-1956, Volume 4, Number 1, pp 19-29

[15] Divya Shrungar J, Priya M P and Asha S M," Fog Computing: Security in Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 8, pp 803-807, August 2015.

[16] http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing
[17]http://www.webopedia.com/quick_ref/cloud_computing.asp
[18] Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan. 2014.
[19] Shanhe Yi, Cheng Li and Qun Li," A Survey of Fog Computing: Concepts, Applications and Issues", Mobidata'15, June 21, 2015.