International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-6)

Research Article

June 2015

An Analysis of Performance for Multi Tenant Application through Cloud SIM

Bhawna Sehgal
Mtech Student (C.S.E)
H.E.C Jagadhari
Kurukshetra University
Haryana, India

Er. Jasbeer Narwal
Assistant Prof. (Mtech)
H.E.C Jagadhari
Kurukshetra University
Haryana, India

Abstract:

The capability to scale a web application or website is tied directly to understanding where the resource constraints lie and what Affect the addition of various resources on the application. Unluckily, architects more often than not assume thatsimply adding another server into the mix can solve any performance problem and security problem. Cloud is a platform shufflethat enables a fierce and argumentative debate on the issues of security and performance surrounding how to secure information and instantiate trust in an open and assumed-hostile web operating environment. When you start adding new hardware/update existing hardware in a web cloud, the complexity starts increasing which affects performance and hence security. So, here we will define the algorithms to keep both performance and data secure but flexible enough to allow for expandability.

Keywords: Cloud Platform, Cloud Security, Multitenant, Cloud Sim , Performance evaluation

I. INTRODUCTION

The designers of security solutions have regularly debated the balances between levels of resulting performance security When computational resources are provided to the current system, one of the key challenges that computing community face is leaked security and deteriorating performance. "Cloud computing" takes grasp as 69% of all internet users have either stored data online or used a web-based software application[1]. Growths in the number of applications and the volume of data that must be managed have made data centers to be as wide as possible, with no end in sight. But if cloud computing is going to meet enterprise needs for confidentiality of customer data and acquiescence with legal directives, it will have to provide increased levels of security to support more sensitive enterprise applications. To date, most of the public cloud-oriented applications have been consumer-centered applications built on commoditized data storage and transaction processing. At this initial stage, the applications and data being processed in clouds are mainly non- sensitive, and the cloud services offer minimal or only generally available security. In a web application, you don't simply add more capacity to the system just because your CPUs have hit 90% utilization. It's important to be able to answer the question, "What does supporting this additional load get me?[2][3]" Knowing the value of the demand on your system will help answer that question.

II. CLOUD COMPUTING

Cloud computing is a model for facilitating suitable, on- demand network access to a shared pool of configurable computing resources (e.g. Networks, Servers, Storage, Applications, and Services) that can be quickly provisioned and released with minimal management effort or service provider interaction. This cloud model stimulates availability and is composed of three service models, and four deployment models. However "Cloud computing" is a difficult term to explain to most; even to IT professionals, The "cloud" is defined as the Internet surrounding every part of our daily lives, similar to the clouds in the sky. While a common misunderstanding for cloud computing is only storage space on the Internet, the cloud offers various services, infrastructure benefits which may not be possible within ordinary local-area enterprise networks. When cloud storage is used as the first location of files , a trust is left in the hands of the storage provider to ensure certain steps are taken to prevent data loss and to maintain the integrity of the file system; assisting maximum uptime, reducing downtime and bear the highest levels of physical protection and data security. When something affects cloud storage, things can go unfortunately wrong for many end users. While data which is stored in the cloud isn't actually stored in the cloud; rather a data Center housing hundreds of servers and networking cables, physical disasters are one of the greater threats to the cloud[4].

As physical disasters go, some will distress the entire cloud, or entire datacenter if you think geologically or physically, and some will affect portions or individual sections. Natural disasters are a great concern to those who run and use cloud computing services. As many natural disasters are unpredictable, recovering from these disasters are often impossible. Preventing disasters from affecting the cloud itself is the only faithful thing the staff, management and planners can expect. Nobody would build a datacenter; let alone any Business Venture, Government building, School or Hospital, or any building or structure of importance in a geographic location where an active or inactive volcano lies, e.g. In case of cloud downtime or event which causes the cloud to fail, a backup solution is often used in an alternate location. This

ensures a constant stream of data being backed up to an alternate datacenter, away from any potential natural disaster, but keeping data secure and maximizing authorized accessibility.

III. ARCHITECTURE

After analyzing WBS (Web Banking System), Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, consist of hardware and software designed by a cloud architect who works for a cloud integrator. It involves multiple cloud components communicating with each other over application programming interfaces, usually web services. This resembles the Unix philosophy of having multiple programs doing one thing well and working together over universal interfaces. Complexity is controlled and the resulting systems are more manageable than their uniform counterparts. Cloud architecture extends to the client, where web browsers and/or software applications access cloud
applications.

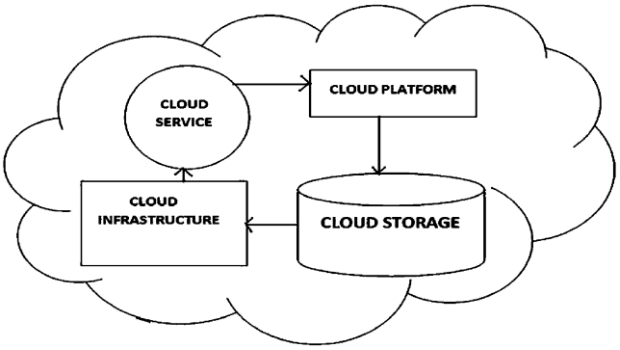

Fig.1: Architecture of Cloud

Cloud storage architecture is loosely coupled, where metadata operations are centralized enabling the data nodes, each independently delivering data to applications or users. Security is the challenge related to cloud computing according to our architecture. The main security concerns include performance, reliability compliance, privacy in interoperability and visibility under virtualization[5][6].
With increasing Business complexity, organizations are looking for innovative business models and technologies to cater to customer demands. Cloud computing technologies can provide organizations competitive advantage in the market, cost reductions, simplified maintenance and management of applications across the enterprise, greatly extended scalability, high availability, automation, large data storages and reliable backup mechanisms.

IV. SERVICE MODELS

Cloud Software as a Service (SaaS). The ability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to providE processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)[14].

V. DEPLOYMENT MODELS

Community Cloud: The Cloud infrastructure is shared by various organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
Public Cloud: The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Private Cloud: The Cloud infrastructure is operated only for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
Hybrid Cloud: The Cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)[13].

VI. CURRENT TRENDS

Critics argue that Cloud Computing is not secure enough because data leaves companies' local area networks. It is up to the clients to decide the vendors, depending on how eagerly they are to implement secure policies and be subject to 3rd party verifications. Salesforce, Amazon and Google are currently providing such services, charging clients using an on-demand policy. Statistics suggest that one third of breaches are due to laptops falling in the wrong hands and about 16% due to stolen items by employees. Storing the data in the cloud can prevent these issues altogether. Moreover, vendors can update application/OS/
middleware security patches faster because of higher availability of staff and resources.

According to cloud vendors, most thefts occur when users with authorized access do not handle data properly. Upon a logout from the cloud session, the browser may be designed to delete data automatically and log files on the vendor side indicate which user accessed what data. This approach may be considered safer that storing data on the client side. There are some applications for which Cloud Computing is the best option[7]. One example is the New York Times using Amazon's cloud service to generate PDF documents of several-decade old articles. The estimated time for doing the task on the Times' servers was 14 years, whereas the cloud provided the answer in one day for a couple hundred dollars.

However, the profile of the companies that currently use the Cloud Technology includes Web 2.0 start-ups that want to minimize material cost, application developers that want to enable their software as a service or enterprises that are exploring the cloud with small applications. The fact that Cloud Computing is not used for all of its potential is due to a variety of concerns. [8][9]

VII. PERFORMANCE ISSUES

Nowadays, everybody seems to be talking loud about Cloud Computing . But the recent reported outages Amazon and Google has made us think and gets surprise if the cloud is really ready to meet all the propaganda and attention its getting. No doubt, there are cost savings related to maintenance and application / server management. But does this certify that your end users are getting the online experience you want them to have[10]?

Many Cloud Computing providers control panels or custom consoles for managing server resources. These consoles provide customers with availability statistics and status messages in the event of important outages that effect end users[11].

VIII. IMPROVE PERFORMANCE & SECURITY ISSUES-EQUATIONS

The first thing to keep in mind is that even you are hosting on a Cloud or have a SAAS app running somewhere, your end user hopes are not different than the regular client server application. So in a common sense user acceptance testing is not much different than testing on a Client Server Architecture[12][15]We know, web based application environment in the cloud is a puzzle of pieces. At the core you have your virtual hardware followed by your operating system. Each of your servers is then designed differently depending on its specific duty. You may have application servers, web servers, search servers, database servers etc.

Each of these servers needs to be observed from various points of view - both internally and externally. Though you don't have direct access to performance observation like in a Client Server Architecture but still you can follow following steps to make sure your users are getting the experience you want them to:

Algorithm at the server side:

Notation:

T_{low} : Time interval for the slow mode
T_{high} : Time interval for the fast mode
T_{fixed} : Fixed time interval for the super-fast mode
T_{th} Threshold time
C_{size} : Cloud size
I_{dr} : id of Resources
gid : group id of Resources
D : the set of Resources
IR : the set of resources ids
$Clients_{th\text{-}low}$: the lower threshold number of clients for the cloud
$Client_{th\text{-}high}$: the higher threshold number of clients for the cloud
R_{data} : an id list of resources that a client has requested from the cloud
$R_{brodcast}$: an id list of data items that the server received in the IR interval; initialized to be empty
$R_{performance}$: Performance of cloud and timestamp for all resources
S_r : Start Resources
S_t : Stop Resouces
Performance: Sr(n)t…St(n)t
Performance: Performance issue = Sr(n)t-St(n)t

(A) Slow Mode (cloud performance)

At interval time Ti, construct IRi, as follows-

IRi= {[gid,t]|(gid) **.**{IR})^((Ti-T_{low}*w)<t<Ti)};

Broadcast IRi, T_{low};
Receive R_{data};
For every idr **.**Rdata broadcast **.**D{
Update Counterclient
Execute Step B if Tth is reached and
Counterclient > $Client_{th\text{-}high}$
}

(B) Fast Mode(cloud performance)
At interval time Ti, construct IRi, as follows-
IRi = {[idt, t]|(idr **.**{IR})^((Ti- T_{high}*w)<t<Ti)};
Broadcast IRi, T_{high};
Receive R_{data};
For every idr **.**R_{data} broadcast **.**D{
Update Counterclient
Execute step A if T_{th} is reached and Counterclient<$Client_{th\text{-}low}$;
Execute step C if Tth is reached and Counterclient>$Client_{th\text{-}high}$
}

(C) Super fast Mode (cloud performance)
At interval time Ti, construct IRi, as follows-
IRi={[d,t]|(d**.**D)^((Ti-T_{fixed}*w) < t <Ti)};
Send IRi. T_{fixed} point to point;
Execute step B after T_{fixed} is elapsed;

IX. RESULTS

Table 1 Result Table of Different Resources Of Cloudlet Through Cloudsim

RAM Size (mb)	Cloudlet ID	Status	Data Center ID	Virtual Machine ID	Time (MIPS)	Start Time (MIPS)	Finish Time (MIPS)	User ID	Debt
512 -2048	0-1	Success	2-3	0-1	160	0	160	3	35.6-112.4
512-2048	0	Success	2-3	0	160	0	160	4-5	36.2-114.7
512-2048	0-8	Success	2	0-4	320	0	320	4-5	5128-5512
512-2048	0-520	Success	3	0-104	320	0-200	320	5-6	5217-5738

X. CONCLUSION

In conclusion, physical or natural catastrophe to the datacenter which houses the cloud in hardware form would be the main matter of concern to the company or those involved in the running of the datacenter. On the other hand, irrespective of company size or volume and magnitude of the cloud, from the findings discussed within this paper, network or computing downtime is the most harmful effect to have on the end user. If you have no connectivity to the Internet or from the Internet to the datacenter where the cloud is hosted, you cannot access what you need to and the whole cloud concept is therefore made redundant.

XI. FUTURE WORK

For those deploying software out in the cloud, security of scalability is a major issue.

1. The need to arrange resources in such a way that a program continues running efficiently even as the number of users grows.
2. It is not just that servers must respond to hundreds or thousands of requests per second.
3. The system must also manage information coming from multiple sources fast, not all of which are under the control, of same organization.

With these equations there is a possibility that the security can be breached, but the performance will be increased according to our scenario when the number of users are increased. In future we want to design a protocol which will be more secure and the performance of the cloud will increase.

REFERENCES

[1] Venkata Narasimha Inukollu, Sailaja Arsi and Srinivasa Rao Ravuri, " Security issues Associated with Big Data in Cloud Computing", May 2014 International Journal of Network Security & its Applications(INSA).
[2] Leena Khanna, Anant Jaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms To Overcome Them ", March 2013 International journal of Advance Research in Computer Science and Software Engineering.

[3] Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz, "Securing Software as a Service Model of Cloud Computing:Issues and Solutions", August 2013 International journal on Cloud Computing:Services and Architecture(IJCCSA).
[4] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenge", March 2012, International Journal of Soft Computing and Engineering(IJSCE).
[5] J.SRINIVAS, K. VENKATA SUBBA REDDY, Dr. A.MOIZ QYSER , "Cloud Computing Basics", July 2012,International Jounal of Advanced Research in Computer and Communication Engineering.
[6] Lijun Mei,W.K. Chan,T.H. Tse, "A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues", 2008 IEEE Asia-Pacific Services Computing Conference.
[7] Hong Cai, Ning Wang, Ming Jun Zhou, "A Transparent Approach of Enabling SaaS Multi-tenancy in the Cloud '', 2010 IEEE 6th World Congress on Services.
[8] Chang Jie Guo, Wei Sun, Ying Huang, Zhi Hu Wang, Bo Gao , "A Framework for Native Multi-Tenancy Application Development and Management''2007 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services.
[9] Zeeshan Pervez, Sungyoung Lee, Young-Koo Lee," Multi-Tenant, Secure, Load Disseminated SaaS Architecture'' Department of Computer Engineering, Kyung Hee University, South Korea.
[10] Jack Brass, "Physical Layer Network Isolation in Multi-tenant Clouds" International Conference on Distributed Computing Systems Workshops 2010.
[11] Pankaj Goyal, "Policy-based Event-driven Services-oriented Architecture for Cloud Services Operation & Management" 2009 IEEE International Conference on Cloud Computing.
[12] Guoling Liu. "Research on Independent SaaS Platform" School of Information Science and Technology Shandong Institute of Light Industry Jinan, China.
[13] Qiang Li, Qinfen Hao, Limin Xiao, Zhoujun Li, "Adaptive Management of Virtualized Resources in cloud Computing Using Feedback Control" The 1st International Conference on Information Science and Engineering (ICISE2009)
[14] MingXue Wang, Kosala Yapa Bandara and Claus Pahl, "Process as a Service - Distributed Multi-tenant Policy-based Process Runtime Governance", 2010 IEEE International Conference on Services Computing.
[15] Enrique Jiménez Domingo, Javier Torres Niño, Angel Lagares Lemos, Miguel Lagares Lemos, Ricardo Colomo Palacios, Juan Miguel Gómez Berbís, **"**CLOUDIO: A Cloud Computing-oriented Multi-Tenant Architecture for Business Information Systems",2010 IEEE 3rd International Conference on.

