International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Virtualization, The Great Thing and Issues in Cloud Computing

Sarvesh Kumar[a*], Suraj Pal Singh[b], Ashwanee Kumar Singh[c,] Jahangir Ali[d]

[ad]Computer Science and Engineering, Lovely Professional University, Jalandhar Punjab
[b]Computer Science and Engineering, Sachdeva Institute of Technology Mathura
[c]Electronics and Communication Engineering, Bhagwant University, Ajmer, India

Accepted 13 March 2013, Available online 1June 2013, **Vol.3, No.2 (June 2013)**

Abstract

Now within IT industry virtualization is used between today's interfaces to abstract different layers from each other when one layer is updated, the others one needs update too. When one layer is defined, the upper and lower layer cannot be used for anything else. One of the Top must's rapidly evolving and widely deployed technologies are server virtualization. Many organizations are already the cost savings from implementing virtualized servers and system administrators love the ease of deployment and management for virtualized systems. In this paper we discuss about some major threats of virtualization and cloud computing and discussed about how Google cloud works and a key management algorithm for security purposes in cloud computing.

Keywords: *cloud computing, virtualization, hypervisors, hyper-safe*

Introduction

Cloud computing is a collection of objects that are grouped together. It is the act of grouping or creating a resource pool that is differentiates cloud computing from all other networked systems. Benefits of pooling resources to allocate them on demand are so compelling as to make the adoption of these technologies as priority. Without resource pooling, it is impossible to attain efficient utilization, provide reasonable cost to users and proactively react to demand. When you use cloud computing, you are accessing pooled resources using a technique called virtualization. Virtualization assigns a logical name for a physical resource and then provides a pointer that physical resource when request is made. Virtualization and cloud computing allow computer users access to powerful computers and software applications hosted by remote group of servers but security are related to data privacy are limited public confidence and slowing adoption of new technology. Virtualization allows the pooling of computational power and storage of multiple computers, which can be shared by multiple users. E.g. Under the cloud computing paradigm, Businesses can lease computer resources from a data centre to operate web –sites and interact with customers without having to pay for the overhead of buying and maintaining their own infrastructure. thus virtualization is a techniques of masking or abstracting physical resources. It increases the utilization and capacity of IT resources, such as servers, networks or storage devices beyond their physical limits. Virtualization simplifies resource management by pooling and sharing resources for maximum utilization and makes them appear as logical resources with enhanced capabilities. Thus in this paper we will discuss about what types of threats involved in hypervisors and Google clouds uses the virtualization technology and a key management algorithm for security issues in cloud.

*Corresponding author: Sarvesh Kumar

Load balancing and virtualization

One characteristics of a cloud computing is virtualized network access to a service. No matter where you access the service, you are directed to available resource. Technology used to distribute service request to resources is referred to as load balancing. Load balancing can be implemented in hardware or in software .It is a optimization techniques, it can be used to increase utilization and throughput, lower latency, reduce response time and avoid system overload. Load balancing systems can use different mechanisms to assign service direction.

New Mechanisms for load balancing: steps for load balancing mechanisms.

Load balancer listens to a network port for service request. When a service request from client or service requester arrives, load balancing uses scheduling algorithms to assign when the request is sent. Typically scheduling algorithms are round robin, weighted round robin and fastest response time.

A session ticket is created by load balancer, so that sub sequent related traffic from the client that is part of that

session can be properly routed to same resource. Without this session record, a load balancer would not be able to correctly fail over a request from the resource to another. Persistence can be enforced using session data stored in a data base and replicated across multiple load balancers.

Problem definition

One of the major threats to virtualization and cloud computing is malicious and software that enables computer viruses or other malware that have comprised one computers system to spread to the underlying hypervisor and ultimately to the system of other customer. In short key concern is that one cloud computing customer could download a virus such as one that steals user data and then spread that virus to the systems of all other customers.

Solution of the above problem

Hyper safe utilizes two components to prevent that from happening. The hyper safe program has a technique called non by passable memory lockdown, which explicitly and reliably bars the introduction of the new code be anyone other than the hypervisor administrator. This also prevents attempts to modify existing hypervisor code by external users.

Hyper-safe uses a technique called restricted pointer indexing. This techniques called initially characterize a hypervisors normal behaviour and then prevents any deviation from that profile. Only the hypervisor administrator themselves can introduce changes to male hypervisor code.

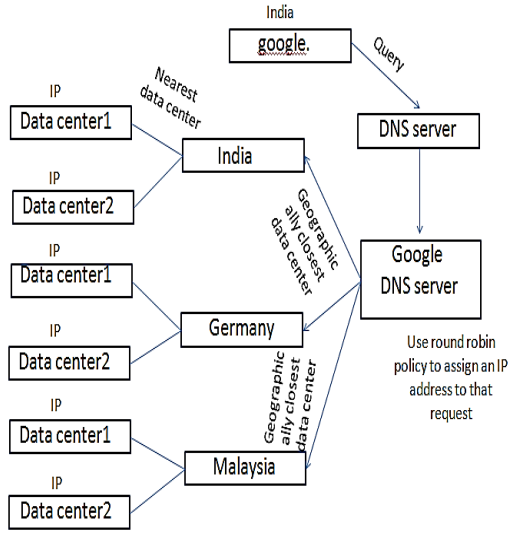
How Google cloud works

Google is the most heavily visited site on the internet. Google has made in infrastructure is enormous and Google cloud is one of the largest in use today. It is estimated Google runs over million server's worldwide, process a billion search requests and generates twenty pega bytes of data par day. Google never gives data center tours to journalists does not disclose where its data center are located. Google has many data centers around the world.

Steps of Google search works

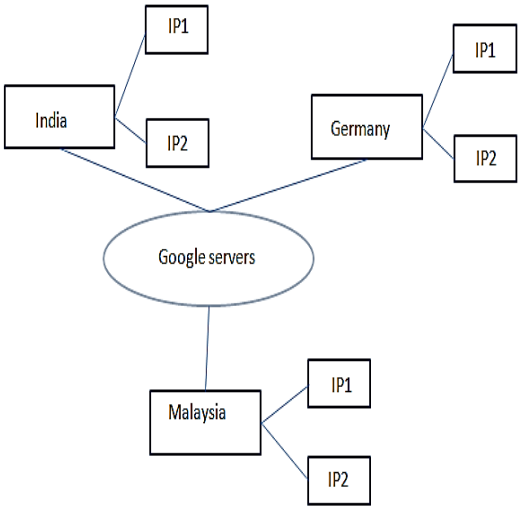
First level of IP virtualization

Google maintains a pool of hundreds of IP addresses. When you initiate a Google search, your query is sent to a DNS server, which then queries Google's DNS server.
The Google DNS server examine the pool determine are geographically origin and uses a round robin policy to assign an IP address to that request. The request usually goes to the nearest data center and that IP address is for a cluster of Google server. This act as a first level of IP virtualization.

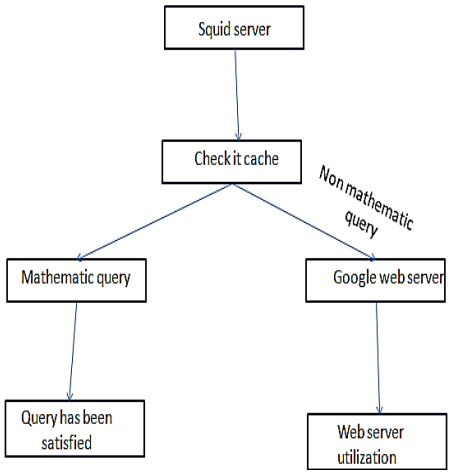


Second level of IP distribution

When the query request arrives at its destination, a Google cluster is sent to a load balancer, which forwards that request to a Squid proxy server and Web cache daemon's. This is the second level of IP distribution, based on measure of the current system loading on servers in the cluster.



C. Third level of IP distribution: The Squid server checks its cache, and if finds a match to the query, that match is returned and the query has been satisfied. If there is no match in squid cache, the query is sent to an individual Google web server based on current web server utilizations which is third level of network load balancing again based on utilization rates.
Google does not use hardware Virtualization, it performs several load balancing to distribute the processing load and to get high utilization rates. The work load management software transfers the work load from a failed server over to redundant server and the failed server is taken offline.



Different types of virtualization

a. **Network virtualization:** it creates virtual networks whereby each application sees its own logical network independent of the physical network. A VLAN is an example of hardware virtualization that provides an easy, flexible and less expensive way to manage network.
b. **Server virtualization:** it enables multiple operating system and applications to run simultaneously on different virtual machines created on the same physical server. it provides a layer of abstraction between OS and underlying hardware.
c. **Storage virtualization:** with storage virtualization, the disk/data storage for your data is consolidated to and managed by virtual storage system. The servers connected to the storage system are not aware of where the data really is.
d. **Application virtualization:** an application runs on another host from where it is installed in a variety of ways. It could be done by application streaming, desktop virtualization or VDI, or a VM package (like VMware ACE creates with a player). Microsoft Soft grid is an example of Application virtualization.
e. **Presentation virtualization**: an application actually runs on another host and you seen on the client are the screen where it is run**.**
f. **Para virtualization:** it requires that the host operating system provide a virtual machines interface for the Guest OS and that the Guest access network through that host virtual machine. an OS running as a guest on a paravirtualization system must be ported to work with the host interface.
g. **Full virtualization:** All OS in full virtualization communicate directly with the VM hypervisors, so guest OS do not require any modification. Guest OS do not require any modification. Guest OS full virtualization systems are generally faster than other virtualization schemes.
h. **Emulation:** Virtual machine simulates network, so it can be independent of the underlying system hardware. A guest OS using emulation does not need to be modified in any way.

Benefits of virtualization

If you are managing multiple servers and desktops, virtualization can help you

1. **Save money:** x86 servers are running at an average of only 20 to 25 percent of total capacity. With virtualization, we can turn a single purpose server into a multi-tasking one, and turn multiple servers into a computing pool that can adapt more flexibly to changing workloads.
2. **Save energy:** Businesses spend a lot of money powering unused server capacities. Virtualization reduces the number of physical servers, reducing the energy required to power and cool them.
3. **Save time:** With fewer servers, we can spend less time on the tasks required for server maintenance. Pooling many storage devices into a single virtual storage device, you can perform tasks such as backup, and recovery more easily and more quickly. It's also much faster to deploy a virtual machine than it is to deploy a new physical server.

Causes of problems associated with cloud computing

- Most security problems are
  - Lack of trust
  - Loss of control
  - Multi tenancy
- These problems exist mainly 3rd party scenario

Loss of control in cloud

a. Consumers loss of control

- Data, applications and resources are located with the cloud provider.
- User id is managed by the cloud.
- User access control and policies is managed by cloud provider.

Security issues in cloud

b. Confidentiality

- Loss of control over data
- The data are stored in cloud are remain confidential.

c. Integrity

- Data is not modified by cloud provider.
- How we ensure that cloud provider is not tampering with our data.

Infrastructure security

- Ensuring confidentiality and authentication of you organizations data from your public cloud provider**.**
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your

organization, or have been assigned to your organization by your public cloud providers.

Local host security

The lack of security of a local host can compromise the cloud and its resources for other users. With mobile devices, the threat may be even stronger, as users misplace or have the device stolen from them. The security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer, providing a potential attacker an easy avenue into a cloud system. If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost.

Conclusion

Thus in this paper we discussed about Virtualization and different types of Virtualization. Virtual memory makes an application appear as if it has its own contiguous logical memory independent of the existing physical memory resource. with technology enhancement, memory technology has changed and the cost of memory has decreased. VMM has evolved enabling multiple applications to be hosted and processed simultaneously. thus this paper focuses on security issues in hypervisors and issues in cloud.

References

I. Foster, Y. Zhao, I. Raicu, and S. Lu (2009), "Cloud computing and grid computing 360-degree compared," *Grid Computing Environments Workshop*, GCE'08, pp. 1-10.

J. Geelan (2008),"Twenty one experts define cloud computing," Virtualization, *Electronic Mag*., article available at http://virtualization.sys-con.com/node/612375.

R. Buyya, C. S. Yeo, and S. Venugopal (2008), "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," *CoRR*, (abs/0808.3558)

Luis M. Vaquero, Luis Rodero-Merino and Daniel Mor´an (2010) "Locking the sky: a survey on IaaS cloud security," *Computing*, DOI:10.1007/s00607-010-0140-x.

Google Docs experienced data breach during March 2009.http://blogs.wsj.com/digits/2009/03/08/1214/

Cloud Security Alliance (CSA) (2009), "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," (Released December 17, http:// www. cloudsecurityalliance. org/guidance/csaguide.v2.1.pdf

Cloud Security Alliance (CSA) (March 2010), "Top Threats to Cloud Computing V 1.0," released March 2010.

The security-as-a-service model. http://cloudsecurity.trendmicro.com/the-security-as-a-service-model/

S.D. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati (2007),"A data outsourcing architecture combining cryptography and access control," Proc. 2007 *ACM workshop on Computer security architecture*, pp. 63-69.

P. Mell and T. Grance (Jan 2011), The NIST Definition of Cloud Computing (Draft). [Online] Available: www.nist.gov/itl/cloud/upload/cloud-defv15.pdf.,

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song (2007), "Provable data possession at untrusted stores," In *ACM CCS*, pages 598-609.

A. Juels and B. S. Kaliski (2007), "PORs: Proofs of retrievability for large files," In ACM CCS, pages 584-597.

Y. Dodis, S. Vadhan, and D. Wichs (2009), "Proofs of retrievability via hardness amplication," In *TCC*.

G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik (2008), "Scalable and efficient provable data possession," *SecureComm*.

C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia (2009),"Dynamic provable data possession," Proc. 16th *ACM conference on Computer and communications security*,pp. 213-222.

K.D. Bowers, A. Juels, and A. Oprea (2009), "HAIL: A high-availability and integrity layer for cloud storage," Proc. 16th *ACM conference on Computer and communications security*, pp. 187-198.

T. Ristenpart, E. Tromer, H. Shacham, and S. Savage (2009), "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," Proc. 16th *ACM conference on Computer and communications security*, pp. 199-212.

V. Sekar and P. Maniatis (2011), "Verifiable resource accounting for cloud computing services," in Proc. 3rd *ACM workshop on Cloud computing security workshop*, 2011, pp. 21-26.

C. Hoff "Cloud computing security: From DDoS (distributed denial of service) to EDoS (economic denial of sustainability)," [Online] Available: http:// www. rationalsurvivability.com/blog/?p=66.

H. Liu (2010), "A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism", *Cloud Computing Security Workshop*.