ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

Virtualization in Cloud Computing

K.S. Kousalyaa Devi[1], S.Gopalakrishnan[2], R.Dhivya[3]

Student, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Dept. of Computer Technology,

Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Student, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[3]

Abstract: Virtualization refers to the act of something including virtual computer makes a unreal image of the storage space devices servers or network resources so that they can be used on multiple machines at the same time. With the latest growth in cloud computing technologies, security of the data becomes important. It is an enable technology allowing the design of an intelligent abstraction layer that hides the density of underlying software or hardware virtualization technology that can make things easier operations as well as allow Information Technology organizations to react faster to changing business demands. It allows multiple virtual computers to run on top of one physical computer and to share the hardware resources, such as printers, scanners, and modems. This increases the efficient use of the computer by low costs since only one physical computer is needed and running. Cloud computing technology is one of the largest milestones in leading us to next generation technology and successful up business and Information Technology field. It helps to rise above the problem for the loss of data, accessing data whenever required and data security. This technology is mainly service oriented and focuses on reduction in low cost, hardware reduction and pay just for service concept.

Keywords: Virtualization, Cloud Computing, Data Security

1. INTRODUCTION

Virtualization is the growing technology in the IT world. It is being used by a growing number of organizations to merge their workloads, to make their IT surroundings scalable and more flexible. In computing, virtualization is the creation of a virtual quite than real report of a resource or device, like a server, an operating system, a storage device or network. It easily provides high availability for critical applications as well as streamlines application use& migrations. It has the capability to run multiple virtual machines on a particular part of hardware. The hardware runs software which enables you to set up multiple operating systems which are able to run simultaneously and independently, in their own secure environment, with minimal reduction in performance. Each virtual machine has its own virtual CPU, network interfaces, storage and operating system. Cloud computing technology is based on three types- grid computing, utility computing and automatic computing. All the data is stored on the servers and can be accessed simply by authenticate with the help of the internet anywhere in the world. Apple, Google, Microsoft, etc. are the major cloud service providers provide very big storage to its users and making the work easier.

2. TYPES OF VIRTUALIZATION

The virtualization has main types are listed below

2.1 Hardware Virtualization

- It is also known as platform **virtualization** refers to the making of actual device that acts like a valid computer with an operating system. It is the concept of computing resources from the software that uses those resources. nowadays, it is often called server virtualization or, simply, virtualization.
- Usage: easier than physical server
- Full: virtual Box
- Para: XEN , KVM

2.2 Software Virtualization

Host machine, Guest machine. A computer on which a hyper visor runs one or more actual machines is called a host machine, and each virtual machine is called a guest machine, Virtual machine manager **(VMM).**Control and monitoring the processor. Operating system level.Operating system virtualization hosting of several virtualized environments within a single OS instance.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

2.3 Storage Virtualization

Several physical storage space devices are grouped simultaneously, which then appear as a particular storage device. The given special return, such as homogenization of storage space across storage devices of several ability and speeds, reduced downtime, weight balancing and improved optimization of act and speed. Partitioning your hard drive into several partitions.Grouping the physical storage from multiple network storage devices so that looks like a single storage devices.

2.4 Data Virtualization

It lets you simply direct data, as the data is exiting as an abstract layer completely independent of data structure and database systems. Decreases in data input and it also formatting the errors.

2.5 Network Virtualization

It several sub-networks can be formed on the similar physical network, which may or may not is certified to communicate with every other. Combining hardware and software network resources and network functionality into a single, software based administrative entity.This enables edge of folder association across networks and enhances safety, and allows improved monitoring and identification of data handling which lets the administrator's level up the network correctly. It also increases reliability as a disturbance in one network doesn't have an effect on other networks, and the analysis is easier.

2.6 Desktop Virtualization

This is perhaps the most frequent form of virtualization for any regular Information Technology employee.The workstation load rather than a server. Allows the user to access the desktop distantly, typically using thin client at the desk. The user's desktop is stored on a distant server, allowing the user to contact the desktop from any device or location. Employees can work expediently from the comfort of their home. Since the data transfer takes position over safe protocols, any threat of data is minimized.

2.7 Why Virtualization?

It can usually develop overall request act due to skill that can stability property and give only what the client needs. One operating system runs the last operating system within program windows.

2.8 Virtualization risk

2.8.1 VM sprawl: Easiness of create VMs, outdated and un patched servers can reproduce in an surroundings.

2.8.2 Sensitive data within a VM: Ease of moving VMs, sensitive data can be compromise.

2.8.3 Security of offline & dormant VMs: The longer a VM is offline, the more it will move away from the safe baseline. If it is current, it may be a important risk for a breech entrance point.

2.8.4 Security of pre-configured (golden image) VM/active VMs: VMs are just archive on the stage, illegal entrance is possible if not suitable security is in place

2.8.5 Lack of visibility and control over virtual networks: Transfer affecting on effective networks may not be able to be seen to usual security safety devices.

2.8.6 Hypervisor security: Illegal access to the hypervisor can occur due to changes in prepared procedure or entrance against physical machines or even actual servers. Functionality used by the admin team may initiate possible safety holes.

3. ATTACKS ON VIRTUALIZATION

Every module of virtualization level can act as an attack vector to initiate more than one attacks on the system. Attacks that aim varies modules of virtualization surroundings may result in protection issues such as cooperate of complete Cloud infrastructure, theft of client information and system hacking. This part discuss about different attack scenarios at virtualization in Cloud.

3.1 Service Provider Attacks

If the hacker has a physical access to the Cloud hardware, hacker may run malicious code in the system to damage the Virtual Machines by modifying their source code and changing their original functionality. With the aid of physical access to the system, hackers can also initiate cross Virtual Machine side channel attacks. These attacks include Control

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

Processing Unit store leakage to assess the load of other virtual web server on the network . Moreover, if the access control is not used properly, different admin such as network admin and virtualization admin might access the client information that they are not official client to access.

These activities will end in security compromise such as failure of data privacy and unauthorized traffic monitoring. Service supplier has to make sure that software deployed on Cloud are built using correct coding practice. Faulty coding can end in web application attacks such as SQL insertion, Cross Site for Scripting, Denial check and Code of Execution. Alert Logic report shows web application attacks to be the most used hackers on Cloud surrounding, impacting more or less 52 percent client.

3.2 Hypervisor Attacks

A Cloud client can lease a visitor Virtual Machine to download a malicious guest OS, which hacks and compromises the hypervisor by changing its source code in order to increase access to the memory inside data and code of VMs present in the system . With further features in hypervisor its better code size has ended in design and implementation vulnerabilities. To manage the entire virtualization environment malicious hypervisors such as BLUEPILL rootkit, Vitriol and are installed on the y, which give hacker the host privileges to alter and control Virtual Machines . This method is used by malicious software to take entire control of the underlying OS by hiding itself from admin and safety software is called hyper jacking.

3.3 Virtual Machine Attacks

Malicious coding in different virtual machines can achieve vital access permissions to follow keystrokes and screen updates across virtual terminal that can be broken by hackers to gain sensitive information. If separation is not properly implemented secret channels can be used for unauthorized person to communicate with other VMs in the system. Attackers can use Trojans, malwares and botnets for traffic monitoring, stealing critical code(data), and tamper the functionality of guest OS. Conficker, Zeus botnet, command and control botnet communication activity are the examples of such attacks that end in data destruction, information gathering and making of backdoors for attackers. Attacks through buggy software, viruses and worms can abuse the guest OS in VMs. Furthermore, unpatched VM OS can be exploited by zero day attacks.

3.4 Guest Image Attacks

Avoidable visitor OS images in Cloud can end result in varies security problems if the security of every image is not maintained. If a malicious guest OS image is migrated to another host, it can compromise the one another system as well. Furthermore, creating too many images and keeping unnecessary images can use resources of the system which can be used as a possible attack vector by attacker to cooperate to the system . When VMs are moved from one physical machine to other, data(code) of VM images might still exist on previous storage space disks that hacker can access.

Similarly, attackers might also recover some data(code) from old disks . The security of image backup is also an problem. By gaining access to the support images hacker can take out all information and data. Hacker can access Virtual Machine checkpoint present in the disk space that contain VM physical memory inside and can expose sensitive information of VM state. A new checkpoint can be created by attacker and load in system to take VM to any desired by hacker. If all the checkpoints in storage space are accessed, data about previous VM states can be obtained .

4. CLOUD DEPLOYMENT MODELS

4.1 Private cloud

It means using a cloud communications (network) exclusively by one client/organization. It is not common with others, yet it is slightly located. If the cloud is on the outside host. The companies have a choice of choosing an on-premise private cloud as well, which is more costly, but they do have a physical control over the communications. The safety and manage level is maximum while using a private network. Yet, the price decrease can be least, if the corporation needs to spend in an on-idea cloud infrastructure.

4.2 Hybrid cloud

It means, using mutually private and public clouds, depending on their idea. For example, public cloud can be used to cooperate with clients, while observance their data secured through a private cloud.

4.3 Community cloud

It implies a communications that is common between organizations, usually with the common data and data managing concerns. For example, it can belong to a administration of a particular country. It can be placed both on and off the premises.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

5. VIRTUALIZATION IN CLOUD COMPUTING

Virtualization in computing is making of virtual (not real) something such as hardware, software, policy or a operating system or a storage or a network device. In this environment Information Technology activity has to handle many changes as the changes arise very fast in effective surroundings than in physical surroundings. Because of not real clouds are scalable and lively. Even though cloud computing can exist without virtualization it may be ineffective and hard As cloud computing tag with pay as you use and endless ease of use these are mainly virtualization idea.

5.1 Benefits of Virtualization Technology

- cost-saving
- hardware-reducing
- energy-saving technique.
- eco-friendly.
- Isolation.
- Resource sharing.
- Aggregation of resources.
- Dynamical resource.
- Consolidation
- Legacy hardware
- Migration
- centralized

5.2 Benefits of Cloud Computing

- Inferior communications and computer expenses for client
- Improved performance
- Fewer Maintenance issues
- Instant software updates
- Improved compatibility between Operating systems
- Backup and recovery
- Performance and Scalability
- Increased storage capacity, data safety

CONCLUSION

To have both physical and not real controls in the environment of cloud computing one must keep data by implementing strong encrypting techniques using protected connections and be valid data loss avoidance policies. Right of entrance control policies are to be recognized and client identity are to be checked. Data middle platforms, communications and client devices are to be safe by trusted computer policies. Allow safe migration from private cloud surroundings to public cloud providers. Without virtualization, cloud computing is achievable but it will be inefficient and hard. It provides flexibility, scalability and low cost advantages to cloud computing. There are many levels and many types to implement virtualization.

6.1 Future Scope

Data loss, data security and difficulty to access the data are some of the key problems that user face but with the use of cloud computing these issues can be determined simply. Some of the main hopes are:

- Relocation time will become insignificant
- Data is safe and data failure is reduced
- One-to-many policy link
- Good check value for computational assets
- Good check quality for computational resources
- Trouble of geographical expanse between user and servers can be avoided
- Band width will be enough for the client
- Data being without a job is reduced

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

REFERENCES

[1]. Swathi T, Srikanth K, Reddy SR (2014) VIRTUALIZATION IN CLOUD COMPUTING, IJCSMC, Vol. 3
[2]. Lombardi L, Pietro RD (2011)
[3]. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Jan, 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145 Cloud Definition.pdf
[4]. "Secure virtualization for cloud computing". Flavio Lombardi, Roberto Di Pietro, June 2010
[5]. Krishnatej K, Patnala E, Narasingu SS, Chaitanya JN (2 Virtualization Technology in Cloud Computing Environment by, IJETAE 3
[6]. Thakral D, Singh M (2014) VIRTUALIZATION IN CLOUD COMPUTING. JCSMC 3:1262–1273
[7]. https://www.omicsonline.org/.../virtualization-in-cloud-computing-2165-7866-10001...
[8]. ieeexplore.ieee.org/document/6138516/
[9]. https://www.ijcsmc.com/docs/papers/May2014/V3I5201499a.pdf
[10]. www.ijstr.org/.../A-Study-On-Virtualization-Techniques-And-Challenges-In-Cloud-Co.
[11]. Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", Int. Journal of Machine Learning and Computing, pp.39-45, vol. 2, no. 1, February, 2012.
[12]. www.fobes.com/cloud computing. [4] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience", 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep.2008, ISBN: 978-0-7695-3352-0
[13]. www.fobes.com/cloud computing
[14]. Orlando, D.: Cloud computing service models.http://www.ibm.com/developerworks/cloud/library/cl-cloudservices1iaas/ cl-cloudservices1iaas-pdf.pdf Last Accessed: 2012-10-27
[15]. Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. Journal of Network and Computer Applications 34(4) (2011) 1113–1122
[16]. Council, V.S.I.G.P.S.S.: Pci dss virtualization guidelines v2.0. (2011) 139
[17]. State of cloud security report: Targeted attacks and real world hacks.
[18]. http://www.alertlogic.com/resources/cloud-security-report/ Last Accessed: 2013-04-14.
[19]. Szefer, J., Keller, E., Lee, R.B., Rexford, J.: Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM conference on
[20]. Computer and communications security, ACM (2011) 401{412