IOP Conf. Series: Materials Science and Engineering **263** (2017) 042002 doi:10.1088/1757-899X/263/4/042002

Efficient operating system level virtualization techniques for cloud resources

Ansu R, Samiksha, Anju S and John Singh K

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: johnsinghaj@yahoo.com

Abstract. Cloud computing is an advancing technology which provides the servcies of Infrastructure, Platform and Software. Virtualization and Computer utility are the keys of Cloud computing. The numbers of cloud users are increasing day by day. So it is the need of the hour to make resources available on demand to satisfy user requirements. The technique in which resources namely storage, processing power, memory and network or I/O are abstracted is known as Virtualization. For executing the operating systems various virtualization techniques are available. They are: Full System Virtualization and Para Virtualization. In Full Virtualization, the whole architecture of hardware is duplicated virtually. No modifications are required in Guest OS as the OS deals with the VM hypervisor directly. In Para Virtualization, modifications of OS is required to run in parallel with other OS. For the Guest OS to access the hardware, the host OS must provide a Virtual Machine Interface. OS virtualization has many advantages such as migrating applications transparently, consolidation of server, online maintenance of OS and providing security. This paper briefs both the virtualization techniques and discusses the issues in OS level virtualization.

1. Introduction

Virtualization is a technology that abstracts the resources from among operating systems and sharing the capability of physical machine by splitting of the resource. It is a one -to -one map between the host operating system and guest operating system. Virtualization can be of two types:
Full Virtualization
Para Virtualization
In Full virtualization, the entire hardware is abstracted so that the operating system would run on the virtual hardware in the same manner as in original hardware. In this guest operating system would run without making any changes to the original source code. It would run independently but it is usually slower in comparison to the Para Virtualization which is operating-system-level-virtualization.
In Para Virtualization, hypervisor is above the physical hardware and host operating system that virtualized the host operating system and guest operating system is at the higher levels. It will allow

modification of guest OS as a result host OS will handle it. It replaces non-virtualized operating system code with virtualized code by "Hyper calls".
VMM (Virtual Machine Monitor) is software component that hosts the guest virtual machines. It lies between the guest operating systems and the physical hardware. This layer abstracts the physical hardware. The technique in which Virtual Machine Monitor does the abstraction is called virtual machine. The abstracted physical hardware is same as running in the VMM. The VMM provides isolation between the multiple instances of virtual machines and provides a single server to run the various machines so as to ensure security services. VMM build on lower level software and provide interface to higher level software. It also manages the memory and scheduling that required to coordinate multiple operating systems. It provides controlled accessing facility for resources shared by the virtual machines. There would be two cases arises, in case if the virtual machine is executed above the Virtual Machine Monitor then it runs any non- privileged instructions directly by virtual machine which will be executed by hardware. And, in case virtual machine runs privileged instruction then an interruption would be generated and then VMM emulate the privileged instruction.
Operating System Virtual Machines will provide an operating system environment in software that run on a single machine. It will support an entire system. This will provide accessing of multiple operating systems on a single machine without rebooting the system as well as it will provide isolated environment for multiple applications.
VM layer has the complete control of the system resources and thus letting security in the VM layer which insures the running of the guest operating system without being aware of the presence of virtualization and easily be running on the top without being compromised by the malware. Both the VM layer and operating system collaborate with each other in order to ensure security in the kernel code and data by enforcing various security techniques.
VMware is a popular tool for virtualization. It provides virtualization by entirely virtualizing the VMM within the hosted operating system. It is referred as the hosted virtual machine architecture. It installed the special operating system driver called VM driver that will allow the virtual machines to provide faster access to the devices on the system. VMware provides generic set of devices to the virtual machines.
The best real world example of using virtualization is in the educational processes. It will provide virtualized environment for the education of engineering in the field of networking. This technique also used in the distributed system and operating system.

2. Literature Survey

The main goal of this paper[1] is to overcome the troubles of specifying the version of the browser, OS, and the number of applications and tools available to the users in order to use the E-learning system. Java Virtual Machine is most commonly used by the E-learning environment but OS virtual machine has lot more advantage over JVM. OS virtual machine will be beneficial for client-server or peer-to-peer E-learning environment. For an Affective Intelligent Tutoring System there are many additional requirements other than the normal pc such as specific drivers for interfacing with the hardware, software which can be made useful in identifying the users, his gestures and the facial features. This software is designed in such a way that it identifies the emotional stage of the user, ie, student based on multiple input output devises and the tutor will also be showcasing artificial emotions to communicate effectively with the user. The devices ranges from normal I/O devices to special devices with which blood pressure, temperature, heartbeat can be measured. Despite having many advantages the installation of drivers is a hideous task. In this paper it is clearly shown that when using a fully virtualized guest OS there is degradation of performance but it is acceptable for the intelligent learning environment. Copying disk images, in this system, during deployment is slow when the copying is done to the local hard disk. SAN approach is recommended for this system. It is identified that there are overheads such as network and file overheads. But this approach is very much suitable

when traditional approaches are used for e-learning in client-server or peer-to-peer environment. This paper states that the overhead for the virtualized I/O can be reduced as the hardware support is more.

This paper [2] states that even though cloud computing works without virtualization it can work better combined with it. This paper also discuss in detail about the different components in virtual environment as well as the different types of virtualization. The paper proposes 3 ways of client virtualization. The first one being server centralized and is controlled by the user. Second one in which the virtual environment will be running on the neighbouring machines. Third one offers different ways to run an application. "Types of security threats find in virtualization are virtual machine threat, hypervisor threat, virtual infrastructure and virtual network threat." In cloud environment it is the responsibility of the "cloud service provider to ensure that the deleted data are not recovered." To maintain the platform specific state and caching level of different system SIGAR can be included in the hypervisor which will effectively balance processor load. This paper also compares various hypervisor based on virtualization types as well as the Sequential read and Sequential Write.

This paper [3] discuss the various type of virtualization namely server virtualization, full virtualization, para-virtualization, application virtualization, resource virtualization, storage virtualization, desktop virtualization, network virtualization. According to the paper the virtualization challenges are management and security.

This paper [4] tries to bring up how the virtualization can be used to improve the elasticity of the resources in a cloud environment. This paper also tries to give a review about open source virtualization technique.

According to this paper [5] the most challenging task is to identify the capacity plan for the virtual machine. The physical hardware is being managed by the Virtual machine manager and the VMM is not bothered about the work each VM under it is doing. To implement application aware resource manager upper management layer should be able to free VMM.

"Virtualization can improve [6] flexibility of the system by running the application OS and a real-time OS (RTOS) on the same processor in parallel. Operating System Level Virtualization can be provided by the hypervisor, L4 microkernel."

The application OS can be used for systems where distribution of applications is required. But it support the features of Real Time Operating Systems (RTOS). In RTOS, applications cannot be developed. So to avoid the drawbacks of both the operating systems, the technique called virtualization can be used. Both of these Operating Systems can be run as Guest Operating Systems (Guest OS) with one hypervisor.

L4 microkernel was developed by German Computer Scientist JochenLiedtke. It comes under the second generation family of microkernels. It provides Operating System Virtualization and it is an effective hypervisor.

The architecture for virtualization of Linux kernel based on L4 microkernel is proposed. In order to virtualize the Linux kernel, features like Exception handling, interruption handling, scheduling, memory management, etc. must be modified.

L4 microkernel works depending the threads and address spaces. Thread is executed inside the address space and address spaces are constructed and maintained recursively by user level servers, called pagers. It is developed by three basic operations known as, granting, mapping and un mapping flex pages ie., logical pages. It is secure as it works on virtual pages rather on physical pages.

"Upon booting, L4 microkernel must load the virtualized Linux server process which is a single process. Virtualized Linux does not support features like system call, exception & interruption handling, so L4 microkernel should deal with it. To deal with it, L4 microkernel makes use of two threads namely, exception and interrupt thread internally so as to send Inter Process Communication message to respective threads in Linux server.

Various drawbacks of high level APIs required for developing application, real-time performance & legacy support can be rectified by virtualization. Virtualization improves the flexibility of the system by allowing application OS (Linux, Windows, Symbian, etc) & Real-Time OS (RTOS) run on the same processor in parallel.

If the hypervisor detects the interruption and delivers it to RTOS then RTOS can execute the legacy stack and thus enabling the real-time feature of the device. The application OS provides appropriate API and high-level functionality which is required for developing application. L4 kernel can be use as hypervisor and can be used to provide virtualization in OS. To provide virtualization, Linux Kernel should be modified and features like Exception & Interruption Handling, Memory Management and Scheduling must be taken into account."

"There are two overhead [7] in OS-level virtualization such as start-up and run-time, but it is small compared to the HAL-based virtualization. So it becomes an essential block in developing fault tolerant and intrusion tolerant applications. While creating/ running/ shutting down a Virtual Machine, there is little or no overhead. Windows services like Remote Procedure Call Server Service (RPCSS) has to be virtualized in order to implement OS-level Virtualization. Virtualizing Windows system is a tough task. At the system call interface, the system resource is virtualized by the OS-level virtualization. It depends only on one kernel to allocate system resources to more than one virtual machines which are being executed on OS-level virtualization layer. In the Windows OS, some user-level services are integrated in the kernel. By doing so, we are not able to clone or virtualize each Virtual Machine."
OS-level Virtual Machines can distribute many resources depending on their capability, with other Virtual Machines. We can implement OS-level virtualization by changing the name of the system utilities, so that they are located in a separate name space & intercept the system call interface. The main drawback of OS-level virtualization is that they are not capable to virtualize the kernel state. There are some user-level services in Windows which are very similar to daemons in UNIX OS. Such as Inter Process Mechanisms like COM, DCOM, RPC are handled by RPCSS service.
"It is not easy to virtualize Windows OS because the kernel does not allow some services like RPCSS to be cloned. Windows OS does not allow users to create, register & execute more than one instances of the same system service run in parallel in one Operating System. To clone services provided by Windows, some changes are required to be performed, viz., intercept and modify IPC, inter-service co operations and manipulations in registry.
Virtualizing a Windows OS has 4 steps namely, (1) cloning a Windows Service in Service Control Manager (SCM) logically, (2) cloning a Windows Service by creating a new process and loading it into its appropriate Virtual Machine physically, (3) identifying and modifying inter-service co-operations, (4) picking out and modifying names of system resources."
Feather-weight Virtual Machine (FVM) allows more than one isolated execution environments to run on one Windows kernel. It virtualizes very few number of ordinary services but not able to virtualize other system services like RPCSS and complex services like IIS service group. Virtual Dedicated Server or Virtual Private Service, a machine sold as a service by Internet hosting service, environments are provided by Virtuozzo. It does not provide virtualization of windows service.

Virtualization can be used to create virtual network laboratories [8]. Theselaboratories help in doing researches and experiments in networking. It can also be used for education purposes by the engineers. This paper shows how virtualization can be used in virtual laboratory in operating systems course.
To improve one's programming skills, one must run the programs and must monitor the performance of computer. But this may lead to system crush and difficulty in teaching. Here we can make use of virtualization concept. Programs are tested in a virtualized environment. Many applications provides this facility such as VMWare, Virtual PC, Xen, User-mode Linux, etc and can be done on many platforms like Linux and Windows.
Here, they made use of Windows XP to provide virtualization. Microsoft Visual C++ tool is used as the development tool. Microsoft Virtual PC s/w is used for the laboratory. Windows XP is used as Guest OS, ie., OS running on virtual machine. .vmc and .vhd are the two files in which virtul machine is placed. .vmc is a configuration file and .vhd is a virtual disk file. 1GB is the size of .vhd file and 200MB is the limited virtual memory size.

Components like processor, paging file and memory usage are calculated, data are logged and analysed. EatMemoryThread is a function that implements all threads. Memory is allocated, processed but doesnot free memory. So to avoid this, the program starts MemoryStatusThread before allocating memory to threads. It monitors the usage of memory.
To teach operating system concepts, using virtual machines is highly efficient, especially when complicated topics are to be taught. The drawback was accuracy. It could not provide accurate results of memory usage because the threads which measures the memory status also consumes memory. There is no mechanism to measure the usage of system automatically.

Reasons for overhead of Type II VMMs are studied [9]. By modifying or extending the host OS can make the Type II platform better for running a virtual machine monitor.
Virtual Machine Monitors running on a Host Operating System are very simple but they have a drawback of execution time. It is very slow compared to the VMMs that are directly built on the hardware.
The reasons for this drawback ie., performance overhead are: (1) main guest machine can be controlled by a separate user process, so host OS needs a separate process for the same. This will lead to many host context switches. It can be overcome by taking few lines of code which controlled the Guest OS and putting into the Host Kernel. (2) Changing Guest Kernel and Guest user space frequently requires huge memory operations on the host. It can be overcome by modifying the segments bounds of host user. (3) Changing two Guest application process requires huge amount of memory mapping operations. It is overcome by using one host to maintain all address space definitions. To do this, 510 lines of code was added to the host kernel.

3. SCOW: Security in Copy-On-Write Mechanism

SCOW: Security in Copy-On-Write Mechanism is our proposed work. In our proposed work, we are trying to provide Security in Copy-On-Write mechanism.
Copy-On-Write (COW) mechanism helps in sharing of resources in cloud environment by making duplicate copies of modifiable resources. It is also known as implicit sharing or shadowing. At first, copy of the resource will be created then a write is performed, so the name depicts Copy-On-Write. It decreases the usage of resources by unmodified copies but increases the overhead of resource-modifying operations.
Feather-weight Virtual Machine (FVM) is an Operating System level virtualization technique for Windows Operating Systems. FVM uses Copy-On-Write mechanism for storage of file system. It is easy to back-up, less space consumption, easy to cache on comparison to block level copy-on-write.
In our work, we are using Certificate Authority (CA) instead of Public Key Authority to overcome the bottlenecks of the system. In order to communicate with other users, each user must contact the Public Key Authority to access the public key of other users.
Every certificate consists of three parameters: user's ID, user's public key and a certificate signed by the trusted third party i.e., Certificate Authority.
Steps:
1. Sender requests the certificate authority, for a certificate by providing his/her public key.
2. CA receives the request of public key provided by the sender.
3. CA provides the certificate by encrypting it with Private Key used by the authority.

$$C_A = \mathrm{E}(PR_{\mathrm{auth}}, [T||ID_A||PU_a])$$

4. FVM checks whether the certificate is authenticated from CA.
5. The sender pass this certificate to the receiver who reads and verifies the certificate as follows:

$$\mathrm{D}(PU_{\mathrm{auth}}, C_A) = \mathrm{D}(PU_{\mathrm{auth}}, \mathrm{E}(PR_{\mathrm{auth}}, [T||ID_A||PU_a])) = (T||ID_A||PU_a)$$

6. Receiver is also authenticated in the same manner as sender.

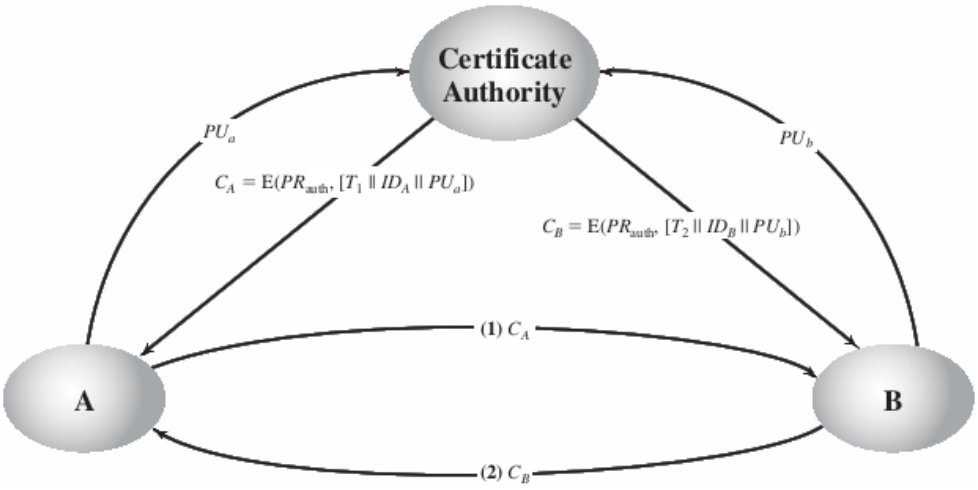

Figure 1. Obtaining Certificates from CA & Exchanging Certificates

4. Result Analysis

We achieved the three triads of network security ie.,Confidentiality, Integrity and Authentication from our proposed system. By using public key and private key concepts we achieved Confidentiality. Only the authorized users are allowed to make changes in the file, thus we achieved Integrity. We achieved authentication by using timestamp which acts as an expiration date. For example, the attacker gains the access of sender's private key. Then the sender creates a new public/private key pair and again requests for new certificate to the CA. In between, if the attacker uses the old certificate and contacts receiver before the sender receives the new one, then receiver encrypts using the old public key and attacker will be able to read the message. Timestamp is used to overcome this scenario.

References

[1] Messom C, Sarrafzadeh A, Gerdelan A, Johnson M and Shanbehzadeh J 2007 Operating system virtualization to support e-learning with affective intelligent tutoring systems *In Innovations in Information Technology 4th International Conference on IEEE* 143-147
[2] Mateen A and Waheed A 2016 The Role of Virtualization Techniques to Overcome the Challenges in Cloud Computing *In International Journal of Computer Applications* **143**
[3] Singh B, Singh J, and Kumar S Virtualization Techniques and Virtualization Challenges in Cloud Computing: A Review
[4] Sharma T and Jarged S 2016 Virtualization Techniques In Cloud Computing *Imperial Journal of Interdisciplinary Research* **2(5)**
[5] Rodríguez-Haro F, Freitag F, Navarro L, Hernánchez-sánchez E, Farías-Mendoza N, Guerrero-Ibáñez J A and González-Potes A 2012 A summary of virtualization techniques. Procedia Technology **3** 267-272
[6] Kim D G, Lee S M and Shin D R 2008 Design of the Operating System Virtualization on L4 Microkernel *In Networked Computing and Advanced Information Management Fourth International Conference on IEEE* **1** 307-310
[7] Shan Z, Chiueh T C, and Wang X 2011 Virtualizing system and ordinary services in Windows-based OS-level virtual machines *In Proceedings of the 2011 ACM Symposium on Applied*

Computing ACM 579-583
[8] Dobrilovic D and Stojanov Z 2006 Using virtualization software in operating systems course *In Information Technology: Research and Education International Conference on IEEE* 222-226
[9] King S T, Dunlap G W, and Chen P M 2003 Operating System Support for Virtual Machines *In USENIX Annual Technical Conference General Track* 71-84