 The Open Cybernetics & Systemics Journal, 2015, 9, 350-358

A Survey: Main Virtualization Methods and Key Virtualization Technologies of CPU and Memory

Shukun Liu[1,2,*] and Weijia Jia[3]

[1]School of Information Science and Engineering, Central South University, Changsha, 410083, P.R. China; [2]School of Information Science and Engineering, Hunan International Economics University, Changsha, 410205, P.R. China; [3]Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China

Abstract: As the core foundation of cloud computing and big data, virtualization technology has become more important now. From the view of development of virtualization technology, a basic discipline and a definition of virtualization are introduced in this paper. And from the perspective of system virtualization, the main classification of virtualization is also discussed in the paper . Proper virtualization methods and virtualization technologies are the key factors responsible for the success of different virtualization. Based on the level of hardware, hardware-aided methods, such as Intel-VT and AMD-V are explicated. The concrete demonstrations of full virtualization, para-virtualization and hardware-aided virtualization in the paper are explicated in detail. The key virtualization technologies of CPU, memory and I/O are also demonstrated. In order to satisfy different requirements of users, for example, work, personal, and geographic mobility needs, more people carry different phones, because of raw embedded virtualization technology these days. Therefore, some primary challenges of virtualization technology in embedded field are discussed in the end of this paper as well.

Keywords: Architecture, Performance, Virtual machine monitor, Virtual machine, Virtualization.

1. INTRODUCTION

Nowadays cloud computing and big data are all hot research issues and virtualization technology is the basic foundation of these concepts. As a result of constructing an isolated computer system, the sharing rate and availability of devices can be improved greatly [1].

In the early 60th century, research on virtualization technology had already begun. From the development of memory virtualization, java virtualization and system architectures of X86 to the virtualization of all kinds of resources, all of them have brought new connotations to virtualization technology [1-3]. In recent years, the academia and industry have paid more attentions to virtualization technology. With the development of a variety of terminal equipment, embedded virtualization has also gradually become a hot issue . In future, virtualization technology will have broad application prospect and wide theoretical value.

2. JUDGING STANDARDS OF VIRTUALIZATION

The essence of virtualization is that real environment program or component can run in a virtual environment. The computer system can be divided into several levels, for example, hardware level, operating system level, application programming interface level and so on. Among the hierarchical structures, virtual levels can be constructed with virtualization technology. The similar or the same functions can be provided to the upper level of low level [4, 5]. Virtualization technology weakens the close relationship between the upper level and lower level. The operation of upper level does not depend on specific physical implementation of the lower level. The typical advantage is that the coupling relationship between the upper and lower level can be removed [4, 5].

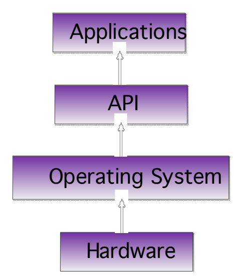

Fig. (1). Virtual level structure.

2.1. Definition of Virtualization

Virtualization can create virtual edition of many things, for example, operating system, computer system, storage and network resources. Virtualization can supply general and abstract interfaces, so that the differences of the attributes and operations can be kept hidden. The resources can be managed conveniently (Fig. **1**).

2.2. Virtualization Principles

There are many standards of virtualization technology. But the mainstream principle was proposed by G.Popek and R.Goldberg in 1974. A virtual machine monitor needs to

*Address correspondence to this author at the School of Information Science and Engineering, Central South University, Changsha, 410083, P.R. China; Tel: +86 15116243570; Fax: +86 731 88144883;
E-mail: liu_shukun@163.com

1874-110X/15 2015 Bentham Open

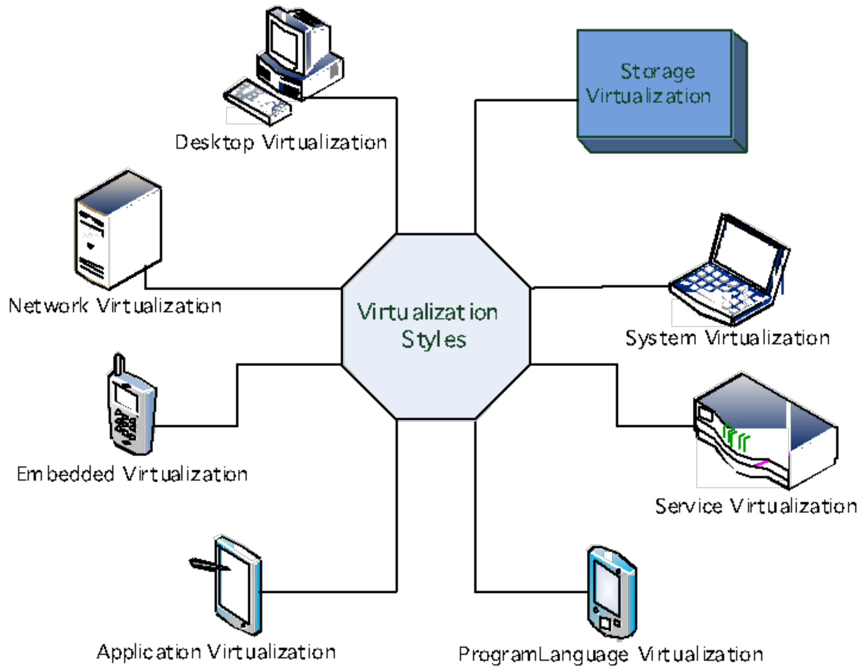

Fig. (2). Virtualization styles.

exhibit three properties in order to correctly satisfy their definition:

(1) Fidelity. The environment it creates for the VM is essentially identical to the original (hardware) physical machine.

(2) Isolation or Safety. The VMM must have complete control of the system resources [6, 7].

(3) Performance. There should be little or no difference in performance between the VM and a physical device [6].

In virtualization environment, virtual resource not only includes all kinds of hardware, but may also contain all kinds of software resources. Virtualization technology can be used for decoupling the close relationship between resource and its users. And users need not depend on the specific implementation of resources at all (Fig. **2**).

3. MAIN TYPES OF VIRTUALIZATION

With the development of computer system, the performance of system will become stronger than before. At the same time, many problems will also emerge. For example, the management of computer system will become more complex. And the overhead of hardware and software of system will also be extended.

Today, with rapid development in CPU technology, almost all computer devices (for example, desktop, laptop or mobile terminal) are equipped with multi-core CPU. Lots of resource managements have become more complex, and the redundancy of resources has inevitably increased to a great extent . In addition, user experience has become the main concern. As a result, various services are now gradually changing from computing-centered mode to the user-centered service computing. Users do not need to understand the underlying structure of computers and the complex physical environment [8]. Researchers found that virtualization technology can solve those problems. In virtualization environment, all kinds of resources can be virtualized. According to the type and system level, virtualization can be classified into architecture level, hardware level, infrastructure level, operating system level, software level and high level program language level and so on.

3.1. Instruction Set Architecture Virtualization

In order to run the operating system freely, the original method of virtualization of instruction set architecture involves constructing different instruction sets.

Most of the traditional computer systems or terminal consists of CPU, memory, disk, I/O, bus and other components. The simulator system is of a typical type, for example, QEMU [9], BIRD [10] and VLIW [11]. Simulator can translate the instructions of users into native machine instructions so that machine can identify and implement local instruction set. The advantage of this method is to build a cross platform (Fig. **3**).

3.2. Hardware Virtualization

Hardware virtualization is similar to the virtualization of instruction set. The main character is that the running environment for users is same to the host machine. Using this character, users can run their instructions on host machine. In this way, code translation can be omitted, and at the same time, the performance is also improved .

The virtual machine a prerequisite for virtualization can run some privilege instructions (for example, the operation modifying page table). When privilege instructions are run, a trap operation would occur through which the operation can be trapped into VMM (Virtual Machine Monitor) [8].

Because of CPU and memory, the privilege instructions can be run by unmodified operation in the virtual machine.

When the privilege instruction appears , the trap will occur immediately. Following this, virtual machine monitor will charge all the resources, therefore, every virtual machine is isolated. In the virtual machine environments, CPU can be used to deal with those privilege instructions, and after that running results will be transferred back to the virtual machine. In order to achieve the goals, technology of code scanning and rewritten dynamic instructions are used in almost all business softwares. Because the character of isolation is very important for hardware virtualization (physical is isolated to virtual machine), the hardware virtualization can support different operating systems and applications which is also very easy to be managed by users. Today, the typical system includes VMware, Virtual PC, Xen, KVM and so on [9] (Fig. **4**).

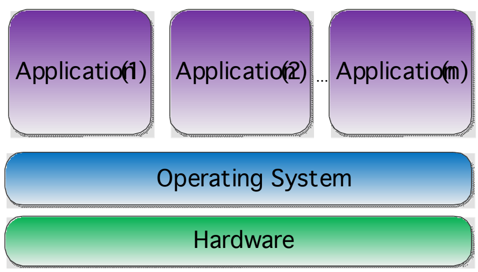

Fig. (3). Typical system structure.

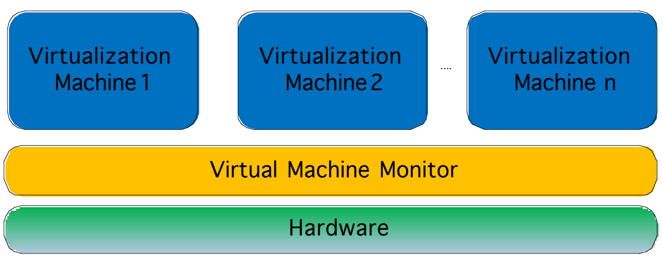

Fig. (4). Typical virtualization system structure.

3.3. Infrastructure Virtualization

Virtualization technology is one of the key technologies in cloud computing which is used to build large data centres. Network and storage are all the foundation of establishing an environment of large data centres.

3.3.1. Network Virtualization

Hardware and software resources can be integrated together which is one of the characteristics of network virtualization. Network virtualization can not only provide the virtual network link to users but also support LAN virtualization and WAN network virtualization.

In local area network virtualization, multiple local networks are combined into one logical virtual network, or a local network is divided into a several logical networks. In order to improve the efficiency of the internal network of large enterprises or data centre, network virtualization technology is used.

3.3.2. Storage Virtualization

Storage virtualization can provide an abstract virtual logic view to physical storage device. Using general logic interfaces which is provided by the logic view, user can integrate all the physical resources together. Storage virtualization can be divided into virtualization based on storage device and network path. Redundant array of inexpensive disks (Raid) is a typical one which is based on the storage device [5-10]. It can implement a high performance disk fault tolerant storage space using number of physical disks.

3.4. System Virtualization

System virtualization is one of the main virtualization technologies. System virtualization can virtualize one physical machine into one or more computer system. Every virtualization system separately has its virtual hardware (such as virtual CPU, virtual memory and virtual I/O devices) and can provide an isolated and undependable running environment [11]. In virtualization system, every computer can run different operating systems, even in undependable environments. Every virtual machine can be in charge of virtual machine monitor. In system virtualization, virtual machine monitor will supply one running environment to the virtual machines which will run in the operating system (Fig. **5**).

In order to achieve system virtualization, virtual machine monitor will have the following characteristics discussed below:

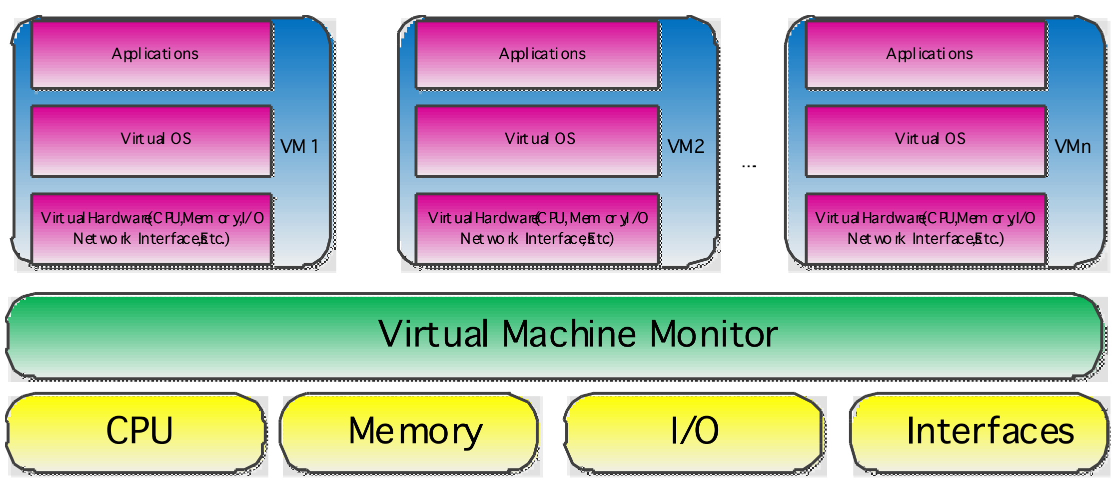

Fig. (5). The concrete typical virtualization system structure.

(1) Control of all resource. That is to say VMM can manage all the system resources.

(2) Equivalence. All the behaviours of the applications (including the operating system), which are managed by virtual machine monitor are similar to the previous ones before they are virtualized except the time sequence and the availability of resources. And prepared privileged instructions can be carried out freely [5, 7, 11].

(3) High Efficiency. Majority of client instructions should be executed directly by the host hardware without the control program participation [5, 7, 12].

3.4.1. Problems of System Virtualization

Researchers have proposed typical system virtualization such as: Privilege-deprivileging and trap-and-emulation. Guest operating system runs in privilege level and virtual machine monitor runs on the highest level. Guest operating system can run non-sensitive instructions, but it experiences trap when running sensitive instructions. Subsequently, the control power will be given to virtual machine monitor which can simulate the running procedure. The preconditions to execute the above process are as follow:(1) CPU must support multiple privilege levels.(2) Non-sensitive instruction execution result should be kept independent of CPU's Privilege level [5-13]. (3) CPU is able to provide a protective mechanism to achieve isolation among physical machines and virtual machines [14]. (4)All sensitive instructions are privileged instructions.

3.4.2. Classification of System Virtualization

In order to overcome the loophole problem of X86 virtualization, full virtualization and para-virtualization have been proposed. Dynamic monitoring method is used in full virtualization technology. Sensitive instructions are transformed into VMM from virtual machine, when they are run. The advantage of this approach is that Guest OS need not to be modified, and at the same time, the disadvantage is that the efficiency is affected by dynamic monitoring. In half virtualization technology, the Guest OS will be modified, the sensitive instructions in VM will be replaced with the VMM hyper call, and the whole process will be completed by VMM. The advantage of this technology lies in the performance of implementation, similar to that of the physical machine while the disadvantage is that the Guest OS will be modified. The two ideas above are based on software system. The former has high efficiency, but it is not user friendly and the latter is convenient for application, but the efficiency is not high. The Intel-VT [7, 13, 14] technology and AMD-V [7, 15-17] technology in the hardware platform for virtual X86 system have provided new hardware foundation which can make up the defects of X86 system virtualization.

3.5. Software Virtualization

In addition to infrastructure virtualization and system virtualization, there exist a virtual environment for software called software virtualization, such as applications and programming languages. This virtualization mainly includes application virtualization and advanced program language virtualization.

3.5.1. Application Virtualization

Application virtualization can decouple applications and operating system, and provide a virtual operating environment for applications. The environment not only includes the application's executable file, but also includes the necessary operation environment needed to for execution. If users need some software, application virtualization server can provide the program and program component in real-time. If client virtualization environment and the application are modified after running, all the modifications will be uploaded to servers [13] and all the servers can dynamically manage resource.

3.5.2. Advanced Program Language Virtualization

Advanced program language virtualization can solve the dynamic migration problems of executable program between different computers (terminals) with different architectures. In the advanced program language virtualization, programs coded with advanced program language can be translated into intermediate instructions which can run using methods of explanation or dynamic binary translation. That is why they can be executed in different architectures systems (Fig. **6**).

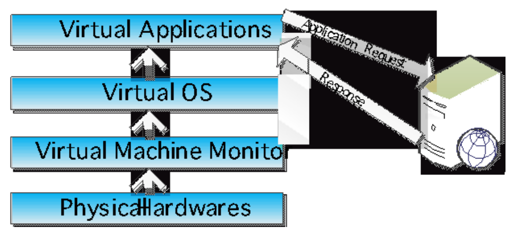

Fig. (6). Advanced program language virtualization.

4. KEY TECHNOLOGIES OF VIRTUALIZATION

CPU, memory and I/O are the main parts of computer. Whether these parts can be virtualized or not is the key factor determining virtualization success.

4.1. Cpu Virtualization

CPU virtualization technology can abstract the physical CPU into virtual CPU. At a time, the physical CPU only executes one virtual CPU instruction. Any user operating system can use one or more virtual CPUs, but in this way all the CPUs are isolated with each other.

The operating system is designed to run directly by hardware. Initially, all the operating systems have the ability to be executed by all the physical devices. They can deal with CPU, use CPU and schedule CPU. There are four levels of CPU in X86 structure. The four levels are level 0, level 1, level 2 and level 3. The highest level is level 0, any command can be executed on it. However, the level decreased from level 1 to level 3. In general, operating system kernel runs at level 0, because it needs to directly modify the state of the CPU, and the general applications run at the level 3 [5, 15, 16].

In order to achieve hardware sharing, virtual level should be added in the operating system with X86 architecture. The virtual level should run at level 0, and user operating system only runs at the levels above the level 0. There are some privilege instructions executed at level 0 of user operating system. Otherwise the meaning of the instructions will change unexpectedly. Because of this situation, it is not easy to virtualize the X 86 systems. In virtual machine, these sensitive instructions do not run on the hardware directly, they will be simulated by virtual machine monitor [9, 17].

In order to solve the problem, full virtualization technology, half-virtualization technology and other technologies such as hardware-aided virtualization were proposed. The problem of privilege instructions in user operating system were solved by binary translation technique and scanning-repair technique.

(1) Binary Translation Technique

The so-called dynamic binary translation technology is based on the process that initially, some privileged instructions are inserted into the trap instruction. When the privileged instructions will be executed in client operating system, they would fall into the virtual machine monitor. Virtual machine monitor will translate the privileged instructions into a series of similar instruction codes and complete these instructions. In the client operating system, these instructions are directly run with codes on hardware. For the non-core instruction, they are run directly by hardware. In fact, the binary translation used by virtual machine monitor is similar to client operating system. An advantage of full virtualization is the implementation of the dynamic instruction [5, 17]. Clients do not need to wait during the running process and client operating system needs not to be changed. The disadvantage is that the performance will be affected by the dynamic translation. For example, full virtualization technique was used in early Micro Virtual Pc and Micro Virtual Server and VMware Station.

(2) Scanning and repair technology

The basic idea of scanning technique is that the instruction blocked will be scanned by VMM before being executed in virtual machine. Through scanning, some sensitive instructions will be detected out, and transferred to the code-patch which is generated by VMM dynamically [18]. Compared with full virtualization, half virtualization technique is also an important virtualization technology which can resolve the problem of privilege virtualization by modifying the client operating system. The operating system which is managed by hypervisor needs to modify its operating system codes to be able to accompany virtual machine monitor to complete its work when it will run some privilege instructions by making use of the interfaces of virtual machine monitor [19]. Xen is one of the typical representatives of para-virtualization technology.

Full virtualization and half virtualization are all software virtualization methods. Both dynamic binary translation technology and hyper call of half virtualization technique belong to software virtualization method. These methods do not change the structure of the CPU. But the performance and efficiency of the entire X 86 systems will be affected.

In order to avoid this problem , some companies such as Intel and AMD have proposed hardware-aided methods for virtualization technology. Using hardware virtualization method can greatly improve the virtualization efficiency. In order to complete the system of CPU associated with the virtual function, new instruction set and processor operating mode are joined in CPU which supports virtualization. Intel-VT and AMD-V are the hardware assisted virtualization technologies. The Intel processor defines two kinds of operation modes: root mode and non-root mode. Virtualization platform runs in root mode, and client operating system runs on non-root mode (Fig. **7**).

4.2. Memory Virtualization

As a new memory management layer, the virtual machine memory management and the classical distinction have many distinctions [5, 20]. The physical memory in virtual machine operating system is no longer the true physical memory, but is the pseudo physical memory which is managed by virtual machine monitor. Corresponding to the "physical" memory is the machine memory. Machine memory refers to the hardware memory. There are three memory types, they are: logical memory, physical memory and machine memory. In virtual memory management system, because of the introduction of the concept of client's physical address, it involves three kinds of memory addresses in virtualization system.(1) Guest Logical Virtual Address (GLVA) is a linear address used by the guest application in OS [20]. (2) Guest Machine Physical Address (GMPA) refers to the physical address used by virtual machine monitor.(3) Host Machine Address (HMA) refers to the real host

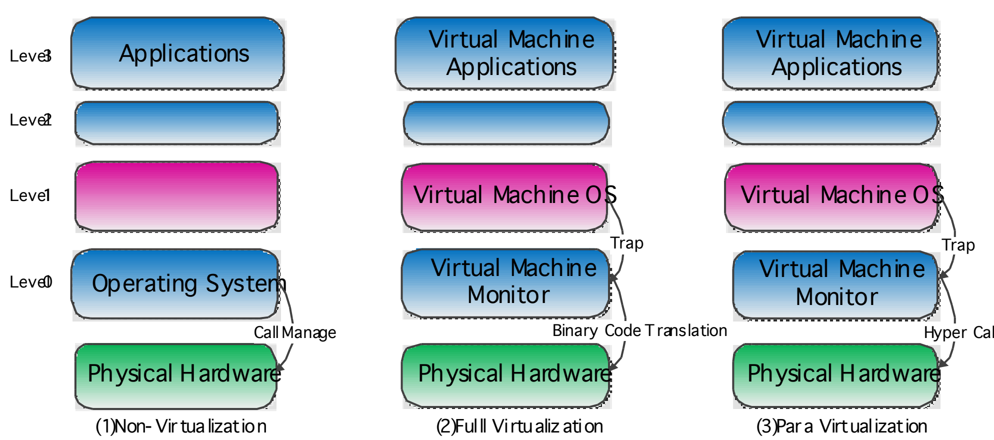

Fig. (7). CPU virtualization types.

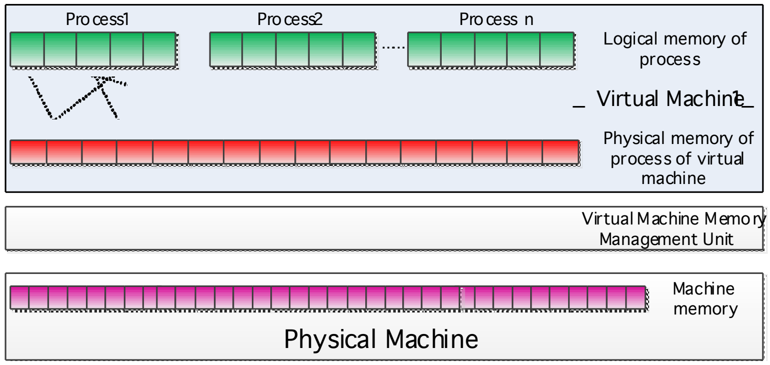

Fig. (8). Memory virtualization level.

physical memory address [20]. Analyzing the relationship of dynamic mapping first (Fig. **8**):

For guest OS, logical virtual address can be seen as a mapping as follow:

GLVA=f1(GMPA) (1)

For virtual machine monitor, the physical address can be seen as a transformation of host machine address:

GMPA=f2(HMA) (2)

Memory virtualization technology paging mechanism mainly uses the MMU class Virtualization (MMU Para virtualization) and the shadow page table.

(1) Class MMU virtualization technology (table write method)

The basic idea of this technique is that when Guest OS creates a new page table, it allocates a page from free space, registered with VMM. Since then, when Guest OS reads or writes the page table, it will fall into the VMM and the VMM will verify the page validity and convert it to a new form. In order to make sure that the Guest OS mapping belongs to its physical pages to virtual machine only, VMM will check the page table. According to the mapping GMPA=f2(HMA), VMM will replace the GMPA of page table with the corresponding HMA. Following this, the page table which is modified will be loaded to MMU. According to the modified page table, VMM can directly map GMVA to HMA. This virtual method needs to modify the Guest OS code [19] (Fig. **9**).

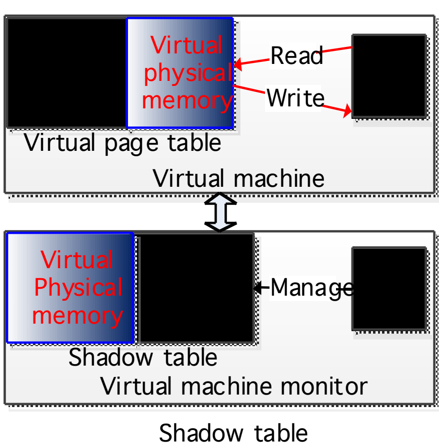

Fig. (9). Shadow table structure.

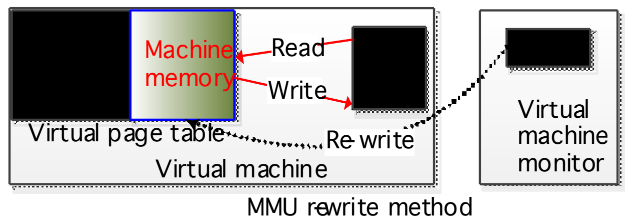

Fig. (10). MMU work method.

(2) Shadow page table technique

Every page table of Guest OS has a shadow page table which is managed by virtual machine monitor with a mapping of HMA=f2(f1(GLVA)) written on shadow page table. The page table of guest OS will maintain its original data. Virtual machine monitor will write the shadow page table into MMU. The technique of shadow page table is used broadly now. Application of shadow page table technology is widely used in VMware Workstation [5], VMware ESX Server and KVM. However, at the same time, shadow page table now is facing the problem of time and space overhead. Therefore shadow page table cache was introduced [20] (Fig. **10**).

4.3. I/O Virtualization

After virtualization of physical I/O devices, the virtualized resources can be provided to different virtual machines. Nowadays, the mainstream I/O virtualization techniques are all implemented by using software methods. Virtualization platform is a sharing platform supporting sharing between hardware and virtual machine. It can provide more convenience to the management of I/O, and make the virtualization resource more abundant. I/O virtualization can virtualize one host physical I/O device into many virtual devices through software simulation. As a result, many virtual machines can multiply the same devices. The method of virtualization is very flexible [5, 21]. It can virtualize the same devices and at the same time it can virtualize different devices. According to different devices, different methods will be used by virtual machine monitor. The commonly used three methods are as follow:

(1) Completely simulation of device interface

In this way, VMM provides the interface definition which is consistent with the actual physical I/O devices. The device simulator of VMM must complete the total simulation of the device's internal interfaces implementation and definition, and can present the same characteristics of real equipment. The virtual machine in this way can directly reuse device drivers without modification of operating system, and can simulate the different physical I/O devices of different hosts. At the same time, it does not need additional hardware overhead. The typical productions of this kind are Microsoft Virtual PC, Orcale Virtual Box and other products [7, 22].

(2) Front end driven /back end driven simulation method

In this way, the front driver (Front-End) is installed on virtual machine, and the back-end drivers are installed in the virtual machine monitor. Front drive which is based on physical drive is simplified, and I/O operations of virtual machine will be transferred to the back end drive by certain means. After being processed, the processing results will be transferred to the front drive. One of the typical products produced by this process is Xen.

(3) Allocation of directly physical devices

Physical devices are allocated to virtual machine directly which eliminates the need of simulation of devices . In the same situation, driven program will be installed in virtual machine. This method of virtualization has high efficiency but the amount of physical devices is limited. The typical productions of the technology are Intel-VT, AMD-d and IOV [23, 24].

4.4. Migration Technology of Virtual Machine

During the process of running virtual machine running, the virtual machine is moved from host machine to the object machine. The running states and the results are not affected by the process. The process is known as the technology of real time migration of virtual machine. Because the resources which are used in virtual machine require mapping, the process of migration is not affected by different architectures of hardware. The online migration technology is the mainstream technique which can degrade the lost performance during the migration process.

In essence, the highly efficient copy of virtual machine is the running states migrating from physical host machine to another physical host machine by computer network through online migration. The running states include resisters of virtual CPU, memory and the states of outside resources (states of disk files and network link). In the environments of LAN, states of outside devices can be deployed by network sharing devices (NAS, NFS). All of these can be used to solve the consistent problem of outside devices of virtual machines.

Therefore, the key problem in online migration of virtual machine is how to solve the high efficiency synchronously. There are three ways of memory migration between physical host machines working in a network.

(1) **Stop running copy**. When VM memory states are copied to the object host, the source host machine will suspend VM. Only when the loading of correct memory state is finished, the VM can be started [7].

(2) **Destination machine's on-demand replication**. Source host machine will suspend VM memory states resided on the source host. Following this, VM resumes in the object host, and accesses the memory pages on-demand from the source host.

(3) **Push mechanism**. Both the source host machine and object machine carry out VM running. During the running process, source end machine push replication of the VM memory state to the destination host voluntarily [5, 7, 25].

5. VIRTUAL MACHINE MONITOR

In virtualization system, Virtual Machine Monitor (VMM) is the most important object. The functions of system are totally dependent on the virtual machine monitor. VMM takes charge of the abstract of the hardware resource and provides the running environments for user operating system. For example, virtual software may achieve the abstraction of hardware, deployment of resource, management, isolation among virtual machines and hosted machines. The virtual level of software is above the hardware platform and below the user operating system. According to the implementation methods, virtual machine monitor can be divided into host way, typical way and hyper way [26].

5.1. Host-based Model

Hosted virtual VMM is an undependable kernel which can run on the host operating system. Using the function of host operating system, hardware resource abstraction and virtual machine management can be achieved. Virtual machine monitor is also an application directly operated on the hardware platform. VMM can manage the resource with the host operating system mechanism. Compared with others, this way is easy to achieve. But the limitation is that all the operation should be participated with host operating system, therefore, the performance may be low. In addition, the security also depends on virtual machine monitor and the hosted machine. The typical instances include VMware Workstation, Microsoft PC and Orcale Virtual Box [9, 22].

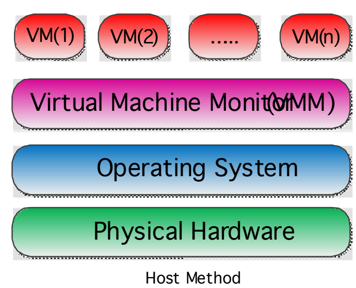

Fig. (11). Hosted machine virtualization.

5.2. Hypervisor Model

Native virtualization is a high performance virtualization technique. In native virtualization architecture, virtual machine monitor runs directly on the hardware (Fig. **11**). It does not depend on the host operating system. The virtual platform directly provides access to the hardware. All virtual clients run on the virtualized platform which provides the instruction set and the device interfaces [27, 28]. All those functions can provide support for virtual machine. This method has a good performance, but the implementation is more complex. The typical instances include Xen, Vmware Esx Server, Microsoft Hyper-v and KVM (Kernel-based Virtual Machine) [9, 25, 29].

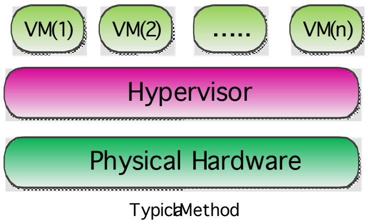

Fig. (12). Typical virtualization method.

5.3. Hybrid Model

In this mode, virtual machine monitor is in the lowest level of the system which manages all the system resources and takes charge of the implementation of virtual machine (Fig. **12**). But virtual machine monitor transfers some control rights of I/O devices to a privilege virtual machine executes on the virtual machine monitor (Fig. **13**). This mode includes all the advantages of above modes. But the disadvantage is that the switch between VMM and privilege operating will bring great overhead [30, 31]. The typical instances of hybrid mode include Hyper-V and Xen.

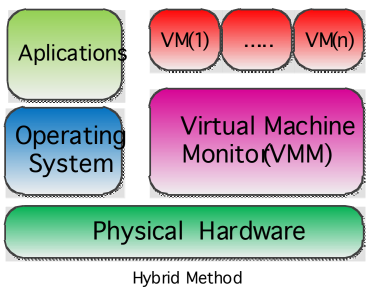

Fig. (13). Hybrid virtualization method.

6. CHALLENGES AND CONCLUSION

Virtualization technology has experienced many eras of development. With the development of cloud computing and big data, one of the big problems in the cloud environments is the deployment and scheduling of virtual machines. Though some related technologies have achieved some progress, the performance and efficiency is very low. Therefore, the problem of deployment and scheduling in cloud is a very difficult problem. With the development of network technologies, the emergence of all kinds of mobile terminals for examples cell phones and pads have brought more conveniences to users [32-35]. The virtualization of embedded devices is a significant problem. Nowadays the virtualization technologies are used for all x86 system.

Because the virtualization of embedded equipment technology is still relatively scarce these days, the hardware structure of embedded devices is diverse and the demand of real time and performance is high, and the challenge of embedded device virtualization is very big. The wide application of virtualization has made the security of virtual machine monitor an important problem. The traditional operating system installed in the antivirus, and the terminal control are not enough to provide physical computer terminal security protection. In order to solve the challenges which virtualizations have been facing, the main researches mainly paying attention to the below facts:

(1) The research of virtualization theory and technology.

This includes basic theory and method of CPU virtualization, memory virtualization, I/O virtualization. For example, the research of scheduling algorithm of different virtual machines in multi-core machine and study of I/O virtualization technology which is aided by hardware are all major focuses of research.

(2) The research of new architecture for VMM.

When hardware assisted virtualization technology was introduced, the loophole problems which is inherent in X 86 systems were solved. In addition, full virtualization technology, para-virtualization technology and hardware assisted virtualization technology were fused together. With the improvement of X86 system, the virtualization technology has made great progress in virtualization itself and its applications. In recent years, the new computing pattern of cloud computing developed greatly, and virtualization is the foundation of cloud computing, therefore its importance and room for development in virtualization is great.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was supported by planned science and technology project of Hunan Province (No. 2014FJ3040), project of China Hunan Provincial Science & Technology Department (No. Math 120236).

REFERENCES

[1] Q. Lin, Z. Qi, J. Wu, Y. Dong and H. Guan, “Optimizing virtual machines using hybrid virtualization, "*Journal of Systems and Software*, vol. 85, no. 11, pp. 2593-2603, Nov. 2012.

[2] Z. Jiong, L. Zixu, H. Yanyan, L. Xiang, “Perspective view of virtualization technologies for avionics system, "*Journal of Beijing University of Aeronautics and Astronautics*, vol. 36, no. 2, pp. 127-130, Feb. 2010.

[3] Z. Weizhe, Z. Hongli, Z. Di and C. Tao, “Memory cooperation optimization strategies of multiple virtual machines in cloud computing environment," *Chinese Journal of Computers*, vol. 34, no. 12, pp. 2265-2277, Dec. 2011.

[4] C. Xiaojun and Z. Jing, “Overview of virtualization technology and its application in manufacturing information," *Computer Engineering and Applications*, vol. 46, no. 23, pp. 25-30, Dec. 2010.

[5] Virtualization and cloud computing group, *Virtualization and Cloud Computing*, Publishing House of Electronic Industry: Beijing, pp. 124-386, 2009.

[6] Y. Wen, J. Zhao, G. Zhao, H. Chen and D. Wang, “A survey of virtualization technologies focusing on untrusted code execution, " In: *2012 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Palermo, Italy, pp. 378-383, 2012.

[7] C. Wenzhi, Y. Yuan, Y. Jianhua and H. Qinmin, “Pcanel/V2 A VMM Architecture based on Intel VT-x," *Chinese Journal of Computers*, vol. 32, no. 7, pp. 1311-1319, Jul. 2009.

[8] N. Penneman, D. Kudinskas, A. Rawsthorne, B. De Sutter, K. De Bosschere, “Formal virtualization requirements for the ARM architecture, "*Journal of Systems Architecture*, vol. 59, no. 3, pp. 144-154, Mar. 2013.

[9] “Qemu cpu emulator,” http://fabrice.bellard.free.fr /qemu /qemu-tech.html, 2004.

[10] S. Nanda, W. Li, L.C. Lam and T. C. Chiueh, “Binary interpretation using runtime disassembly,”http://www.ecsl.cs.sunysb.edu/bird/index.html, 2005.

[11] “Transmeta corp crusoe processor,” http://www.erc.msstate.edu/reese/EE8063/html/transmeta/transmeta.pdf

[12] P. Michael, Z. Sherali and H. Ray, “Virtualization: Issues, security threats, and solutions, "*ACM Computing Surveys*, vol. 45, no. 2, pp. 12-16, Feb. 2013.

[13] T. Guan, J. Hai, X. Xia, C. Wenzhi and Y. Pingpeng, “Measuring and Analyzing CPU Overhead of Virtualization System," In: *Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference*, Jeju, pp. 243-250, 2011.

[14] Z. Yuezhi, Z. Yaoxue, L. Hao, X. Naixue and V. V. Athanasios, “A bare-metal and asymmetric partitioning approach to client virtualization, "*IEEE Transactions on Services Computing*, vol. 7, no. 1, pp. 40-53, Jan. 2014.

[15] C. Chao-Jui, W. Jan-Jan, H. Wei-Chung, L. Pangfeng and Y. Pen-Chung, “Efficient Memory Virtualization for Cross-ISA System Mode Emulation," In: *Proceeding of the 10th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, Szeged, 2014, pp. 117-128.

[16] H. Lv, Y. Dong, J. Duan and K. Tian," Virtualization challenges: A View from Server consolidation perspective," *SIGPLAN Notices*, vol. 47, no. 7, pp. 15-25, Jul. 2012.

[17] S. Foskett, "Virtualization's storage effect server virtualization and enterprise storage, " *InformationWEEK*, no. 1311, pp. 31-34, 2011.

[18] K. Lee, H. Yoon and S. Park, "A Service Path Selection and Adaptation Algorithm in Service-Oriented Network Virtualization Architecture," In: *Proceeding of 2013 International Conference on Parallel and Distributed Systems*, Seoul, pp. 516-521, 2013.

[19] D.F. Bacon, "Virtualization in the age of heterogeneous machines," *SIGPLAN Notices*, vol. 46, no. 7, pp. 11-13, Jul. 2011.

[20] B. Yacine, C. Claude, "Virmanel: A mobile multihop network virtualization tool," In: *Proceeding of the Annual International Conference on Mobile Computing and Networking*, Istanbul, 2012, pp. 67-74.

[21] A. Suzuki and S. Oikawa, "Implementing a Simple Trap and Emulate VMM for the ARM Architecture," *In the proceedings of 17th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, Toyama, pp. 371-379, 2011.

[22] H. Roh, H. Lee and S. Lee, "A study on mobile virtualization”, In: *Proceeding of 16th International Conference on Advanced Communication Technology*," Pyeong Chang, pp. 593-596, 2014.

[23] K. Wang, J. Rao and C. Xu, "Rethink the virtual machine template," *SIGPLAN Notices*, vol. 46, no. 7, pp. 39-49, Jul. 2011.

[24] F. Bingyi, Z. Yunyong, C. Qingjin and J. Xinghua, "Network virtualization technology of cloud computing," *Information Communication Technology*, vol. 50, no. 1, pp. 50-53, May. 2011.

[25] Y. Zheng and W. Li, " A summary of X86-based virtualization technology research," *Journal of Luzhou Vocational and Technological College*, vol. 21, no. 2, pp. 68-73, Feb. 2012.

[26] S. Sharma and M. Chawla, "A Technical Review for Efficient Virtual Machine Migration," In: *Proceeding of 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies*, Washington, pp. 20-25, 2013.

[27] X. Wu, Y. Gao, X. Tian, Y. Song, B. Guo, B. Feng and Y. S. SecMon, "A Secure Introspection Framework for Hardware Virtualization, " In: *Proceeding of the 21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing*, Northern Ireland, pp. 282-286, 2013.

[28] J. Wei, L. Ming-lu and W. Chu-Liang," Security analysis of virtual machine monitor," *Computer Engineering*, vol. 37, no. 15, pp. 116-118, 121, Aug. 2011.

[29] M. Natarajan,"Virtualization of virtual memory address space, "In: *Proc. of The Second International Conference on Computational Science*, *Engineering and Information Technology*, Coimbatore, pp. 732-737, 2012.

[30] Y. Feng, J. Hui, Z. Jian-wei and D. Hai-xin, "Survey on virtual machine environment detection methods," *Journal of Chinese Computer Systems*, vol. 33, no. 8, pp. 1830-1835, Aug. 2012.

[31] Y. Dai, Y. Shi, Y. Qi, J. Ren and P. Wang, "Design and verification of a lightweight reliable virtual machine monitor for a many-core architecture," *Frontiers of Computer Science*, vol. 7, no. 1, pp. 34-43, Jan. 2013.

[32] L. Yong, G. Yudong, W. Xiaorui and S. Guang, "Research and implementation of memory virtualization based on EPT," *Computer Engineering and Design*, vol. 31, no. 18, pp. 4101-4104, Sep. 2010.

[33] X. Wang, J. Zang, Z. Wang, Y. Luo and X. Li, “Selective Hardware/Software Memory Virtualization," *SIGPLAN Notices*, vol. 46, no. 7, pp. 217-226, Jul. 2011.

[34] J. Jeon and T. Han, "Dynamic analysis of virtualization-obfuscated binary executables," *Journal of KIISE: Software and Applications*, vol. 40, no. 1, pp. 61-71, Jan. 2013.

[35] G. Simon, W. Shlomo, "Architectural virtualization extensions: A systems perspective," *Computer Science Review*, vol. 6, no. 5-6, pp. 209-224, Jul. 2012.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014