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

Shukun Liu\textsuperscript{1,2,*} and Weijia Jia\textsuperscript{3}

\textsuperscript{1}School of Information Science and Engineering, Central South University, Changsha, 410083, P.R. China; \textsuperscript{2}School of Information Science and Engineering, Hunan International Economics University, Changsha, 410205, P.R. China; \textsuperscript{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 and more important now. From the view of development of virtualization technology, a basic discipline and a definition of virtualization have been introduced in this paper. And from the perspective of system virtualization, the main classification of virtualization has been showed in the paper also. Proper virtualization methods and virtualization technologies are the key factors of the success for different virtualization. From 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 have been explicated in detail. The key virtualization technologies of CPU, memory and I/O are demonstrated also. In order to satisfy different requirements of users, for example, work, personal, and geographic mobility needs, more and more people have to carry several different phones, because of the raw embedded virtualization technology now. So, some primary challenges of virtualization technology in embedded field have been proposed 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 them. In the way of constructing the isolate computer system, the sharing rate and availability of devices can be improved greatly [1].

In the early 60 century, research of virtualization technology has 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 bring new connotations to virtualization technology [1-3]. In recent years, the academia and industry have paid more and more attentions to virtualization technology. With the development of a variety of terminal equipment, embedded virtualization has gradually become a hot issue too. Virtualization technology will has broad practice application perspective and wide theoretical values.

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 upper level of low level [4, 5]. Virtualization technology makes the close relationship between the upper level and lower level become loose. 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].

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 the differences of the attributes and operations can be hided. The resources can be managed in a transparent way (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 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 may be all kinds of hardware, but also may be all kinds of software resources. Virtualization technology can be used to 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 come out. For example, the management of computer system will become more and more complex. And the overhead of hardware and software of system will become heavier too.

Today, with the fast development of CPU technology, almost all computer devices (for example, desktop, laptop or mobile terminal) are equipped with multi-core CPU. Lots of resources management has become more complex, the redundancy of resources is inevitably increase greatly also. In addition, user experience has more and more concerned. So the various services are now gradually changing from the 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 is constructing different instruction set.

Most of the traditional computer systems or terminal consists of CPU, memory, disk, I/O, bus and other components. The simulator system is a typical type, for example, QEMU [9], BIRD [10] and VLIW [11]. Simulator can translate the instructions of users into native machine instructions. So machine can identify and implement local instruction set. The advantage of this method is to 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 of users is same to host machine. Using this character, users can run their instructions on host machine. So code translation can be omitted, and at the same time, the performance is improved too.

The virtual machine which is needed by virtualization can run some privilege instructions (for example, the operation of modify page table). When privilege instructions were running, a trap operation would occur then the operation can be trapped into VMM (Virtual Machine Monitor) [8].
Because of obtaining CPU and memory, the privilege instructions can be run by unmodified operating in virtual machine. When the privilege occurs, the trap will come out immediately. Virtual machine monitor will charge all the resources. So every virtual machine is isolated. In the virtual machine environments, CPU can be used to deal with those privilege instructions, and then running results will be returned to virtual machine. In order to achieve the goals, technology of code scanning and rewritten of dynamic instructions were used in almost all the business software. Because the character of isolation is very important to hardware virtualization (physical is isolated to virtual machine), the hardware virtualization can support different operating systems and applications. And it is very easy to be managed by users also. Today, the typical system include VMware, Virtual PC, Xen, KVM and so on [9] (Fig. 4).

3.3. Infrastructure Virtualization

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

3.3.1. Network Virtualization

Hardware and software resources can be integrated with together which is one of the characters 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 plurality of logical network. In order to improve 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 by plurality of physical disk.

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 has its virtual hardware (such as virtual CPU, virtual memory and virtual I/O devices) separately and can provide an isolate 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 environments to the virtual machines which will run in the operating system (Fig. 5).
In order to achieve system virtualization, virtual machine monitor will have some characters below:

1. Control 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 same to that before they are virtualized except the time sequence and the availability of resources. And prepared privileged instructions can be free to be carried out [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: Privilege-deprivileging and trap-and-emulation. Guest operating system runs in privilege level. And virtual machine monitor runs on the highest level. Of course guest operating system can run non-sensitive instructions. But when sensitive instructions run, the trap will occur. Then the control power will be given to virtual machine monitor which can simulate the running procedure. The pre-conditions of achieve above are as follow: (1) CPU must support multiple privilege levels; (2) Non-sensitive instruction execution result does not depend on CPU’s Privilege level [5-13]; (3) CPU is able to provide a protective mechanism to achieve the 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 was used in full virtualization technology. Sensitive instructions will be transformed into VMM from virtual machine, when they will be run. The advantage of this approach is that Guest OS need not 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 is similar to that of the physical machine; 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 friendly to users; 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 the 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 is 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 operation environment needed when it will run. 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 dynamic 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 which were coded with advanced program language can be translated into intermediate instructions which can run with the methods of explanation or dynamic binary translation. That is why they can be run in different architectures systems (Fig. 6).

3.6. 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 of virtualization success.

4.1. Cpu Virtualization

CPU virtualization technology can abstract the physical CPU into virtual CPU. At any time the physical CPU only run one virtual CPU instruction. Every user operating system can use one or more virtual CPU, but all the CPUs are isolated with each other.

The operating system is designed to run directly in physical hardware. At beginning of the design, all the operating systems have the ability to visit 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 run on it. The level decreased from level 1 to level 3. In general, operating system kernel runs on level 0, because it needs to directly modify the state of the CPU, and the general applications run on the level 3 [5, 15, 16].

In order to achieve physical hardware sharing, virtual level should be added below the operating system in X86 architecture. The virtual level should run in level 0, and user operating system only run in the levels above the level 0.
There are some privilege instructions which need to run in 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 that 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 that some privileged instruction is inserted into the trap instruction before. 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 instruction into a series of similar instruction codes and complete these instructions. To client operating system, it will feel that it is directly run those codes on physical hardware. For the non-core instruction, they were run directly on physical hardware. In fact, the binary translation is a way of a virtual machine monitor cheating client operating system. An advantage of full virtualization is that the implementation of the dynamic instruction is dynamic [5, 17]. Clients need not waiting during the running process. And client operating system need not be changed. Disadvantage is that 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 instruction block will be scanned by VMM before they run in virtual machine. Through scanning, some sensitive instructions will be detected out, and then they will jump to the code-patch which is generated by VMM dynamically [18]. Compared with full virtualization, half virtualization technique is an important virtualization technology also which can finish the problem of privilege virtualization by modifying the client operating system. The operating system which is managed by hypervisor needs to modify their operating system codes. So it will accompany virtual machine monitor to finish its work when it will run some privilege instructions by call 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 method. Both dynamic binary translation technology and hyper call of half virtualization technique are all 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 above, 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 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 have introduced the hardware assisted virtualization technology. The Intel processor defines two kinds of operation mode: root mode and non-root mode. Virtualization platform runs in root mode, client operating system runs on non-root mode (Fig. 7).

4.2. Memory Virtualization

As a new memory management layer, the memory management 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 by the pseudo physical memory which is managed by virtual machine monitor. Corresponding to the ”physical” memory is machine memory. Machine memory refers to the physical 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 physical address, it involves three kinds of memory address 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 physical memory address [20]. Let us see 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, and registered with VMM. Since then, when Guest OS read or write 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. Then 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 methods need to modify the Guest OS code [19] (Fig. 9).

(2) Shadow page table technique

Every page table of Guest OS has a shadow page table which is managed by virtual machine monitor. And a mapping of HMA=f2(f1(GLVA)) will be written to 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. And at the same time, shadow page table now is facing the problem of the time and space overhead. So shadow page table cache is 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 software methods. Virtualization platform is a sharing platform between sharing 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 by the way of software simulation. So many virtual machines can multiply the same devices. The virtualization way 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 normal 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. In 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, the back-end drivers are installed in the virtual machine monitor. Front drive which is based on physical drive is a 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 front drive. One of the typical products is Xen.

(3) Allocation of directly physical devices

Physical devices are allocated to virtual machine directly. And the simulation of devices is no longer needed. In the same situation, driven program will be installed in virtual machine. According to the method of virtualization, the efficient is most high. But the amount of physical devices is limited. The typical instances of the technology are Intel-VT, AMD-d and IOV [23, 24].

4.4. Migration Technology of Virtual Machine

During the process of virtual machine running, the virtual machine is moved from host machine to object machine. The running states and the results are not affected by the process. The process is called technology of real time migration of virtual machine. Because the resources which are used in virtual machine are resources mapping, the process migration is not affected by the 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 high efficient copy of virtual machine running states from physical host machine to another physical host machine by computer network in the way of 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 if those can be used to solve the consistent problem of outside devices of virtual machines.

So the key problem of virtual machine online migration is how to solve the high efficiency synchronous. There are three ways of memory migration between physical host machines in 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 on-demand replication. Source host machine will suspend VM memory states reside on the source host. Then VM resumed in the object host, and access to memory pages on-demand from the source host.

(3) Push mechanism. Both the source host machine and object machine keep 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 factors. The functions of system are total depend on the virtual machine monitor. VMM takes charge of the abstract of the hardware resource and provide the running environments for user operating system. For example, virtual software may achieve the abstraction of hardware, and 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 run 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 shortage is all the operation should be participated with host operating system, so the performance maybe low. And the security depends on virtual machine monitor and the hosted machine. The typical instances are VMware Workstation, Microsoft PC and Orcale Virtual Box [9, 22].

![Fig. (11). Hosted machine virtualization.](image)

5.2. Hypervisor Model

Native virtualization is a very high performance virtualization way. In native virtualization architecture, virtual machine monitor run directly on the hardware (Fig. 11). It does not depend on the host operating system. The virtual platform directly access to the hardware. Virtual clients all 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 are Xen, Vmware Esx Server, Microsoft Hyper-v and KVM (Kernel-based Virtual Machine) [9, 25, 29].
6. CHALLENGES AND CONCLUSION

Virtualization technology has experienced many periods 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. So 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 into more conveniences to users [32-35]. The virtualization of embedded devices is a hard research problem. Nowadays the virtualization technologies are all for x86 system.

Because the virtualization of embedded equipment technology is still relatively scarce now, the hardware structure of embedded devices is diverse and the demand of real time and performance is high, the challenge of embedded device virtualization is very big. The widely application of virtualization makes the security of virtual machine monitor become an important problem. The traditional operating system installed in the antivirus, terminal control is difficult to provide the physical computer terminal security protection. In order to solve the challenges which the virtualizations have met, the main researches mainly pay attention to 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 research emphasis problems.

(2) The research of new architecture for VMM.

When hardware assisted virtualization technology is introduced, the loophole problems which is inherent in X 86 systems have been solved. And full virtualization technology, para-virtualization technology and hardware assisted virtualization technology are fused together. With the performance improvement of X86 system, the virtualization technology has made great progress in virtualization itself and applications. In recently years, the new computing pattern of cloud computing developed greatly, and virtualization is the foundation of cloud computing, so the importance and developing space of virtualization is immense.

CONFLICT OF INTEREST

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

ACKNOWLEDGEMENTS

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

REFERENCES