A virtual machine monitor (VMM), also called a hypervisor, is the software that securely partitions

the resources of a computer system into one or more virtual machines. A guest operating system is an

operating system that runs under the control of a VMM rather than directly on the hardware. The VMM

runs in kernel mode, whereas a guest OS runs in user mode. Sometimes the hardware supports a third

mode of execution for the guest OS.

VMMs allow several operating systems to run concurrently on a single hardware platform; at the

same time, VMMs enforce isolation among these systems, thus enhancing security. A VMM controls

how the guest operating system uses the hardware resources. The events occurring in one VM do not

affect any other VM running under the same VMM. At the same time, the VMM enables:

• Multiple services to share the same platform.

• The movement of a server from one platform to another, the so-called live migration.

• System modification while maintaining backward compatibility with the original system.

When a guest OS attempts to execute a privileged instruction, the VMM traps the operation and

enforces the correctness and safety of the operation. The VMM guarantees the isolation of the individual

VMs, and thus ensures security and encapsulation, a major concern in cloud computing. At the same time,

the VMM monitors system performance and takes corrective action to avoid performance degradation;

for example, the VMM may swap out a VM(copies all pages of that VM from real memory to disk and

makes the real memory frames available for paging by other VMs) to avoid thrashing.

A VMM virtualizes the CPU and memory. For example, the VMM traps interrupts and dispatches

them to the individual guest operating systems. If a guest OS disables interrupts, the VMM buffers such

interrupts until the guest OS enables them. The VMM maintains a shadow page table for each guest

OS and replicates any modification made by the guest OS in its own shadow page table. This shadow

page table points to the actual page frame and is used by the hardware component called the memory

management unit (MMU) for dynamic address translation.

Memory virtualization has important implications on performance. VMMs use a range of optimization

techniques; for example, VMware systems avoid page duplication among different virtual machines;

they maintain only one copy of a shared page and use copy-on-write policies whereas Xen imposes total

isolation of the VM and does not allow page sharing. VMMs control the virtual memory management

and decide what pages to swap out; for example, when the ESX VMware server wants to swap out

pages, it uses a balloon process inside a guest OS and requests it to allocate more pages to itself, thus

swapping out pages of some of the processes running under that VM. Then it forces the balloon process

to relinquish control of the free page frames.