II[nd] Mid Term Exam Session 2017-18 Subject: Cloud Computing (VII CSE-B)

Q1. What is Virtualization? Differentiate between Server and Desktop virtualization?

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources". In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware. The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine.**

Differences between Server and Desktop Virtualization:

Desktop virtualization separates the software from the physical thin client device. This enables users to access applications and data over different devices and remotely, if they cannot make it into the office. If a device is lost or stolen, IT has the ability to remotely erase any company data from the device. Desktop virtualization will give employees flexibility within their work day. With all of the software and applications not solely stored on a single device, disaster recovery is another major benefit of desktop virtualization.

Server virtualization divides a physical server into separate, smaller virtual servers. This helps maximize a company's resources. Day to day production will run smoother by virtually storing a server, up-time will be increased, and it will be easier to recover from sudden server outages. This will improve server utilization and can even reduce the number of servers a company needs to use to run their programs. With fewer servers, costs are reduced in server maintenance along with power and cooling costs.

Server virtualization does not add any additional load to the network; desktop virtualization operates entirely on the network, which can slow down production speeds. Desktop virtualization requires a company to make more changes in their IT resources. To properly enable desktop virtualization it will affect the data center, network and transmission protocol. Server virtualization only requires changes to be made to the server.

Both desktop virtualization and server virtualization can help cut costs while making data easily available to employees. If a company is considering desktop virtualization or server virtualization they must fully understand the difference between the two. For a smooth transition a company must plan out their move to desktop virtualization, server virtualization or both.

Q2. What are the Security Policies for Cloud Computing?

Definition: In cloud computing , the word cloud is used as metaphor for the “internet” , so the phrase cloud computing means service such as servers are delivered to an organization’s computer and devices through internet.

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

PHYSICAL SECURITY:

Physical security has three important components: access control, surveillance and testing. Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

PERSONEL SECURITY:

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.

Q3. What is BCP (Business Continuity Planning)? Explain.

A business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event. The BCP should state the essential functions of the business, identify which systems and processes must be sustained, and detail how to maintain them. It should take into account any possible business disruption. With risks ranging from cyber-attacks to natural disasters to human error, it is vital for an organization to have a business continuity plan to preserve its health and reputation. A proper BCP decreases the chance of a costly outage. While IT administrators often create the plan, the participation of executive staff can aid the process, adding knowledge of the company, providing oversight and helping to ensure the BCP is regularly updated.

A business continuity plan (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions. Businesses need to look at all such potential threats and devise BCPs to ensure continued operations should the threat become a reality.

A business continuity plan involves the following:

1. Analysis of organizational threats
2. A list of the primary tasks required to keep the organization operations flowing
3. Easily located management contact information
4. Explanation of where personnel should go if there is a disastrous event
5. Information on data backups and organization site backup
6. Collaboration among all facets of the organization
7. Buy-in from everyone in the organization

Q4. Write short notes on (any one)

a. VMware hypervisor

VMware ESXi (formerly **ESX**) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS); instead, it includes and integrates vital OS components, such as a kernel. The VMware vSphere Hypervisor is a free, bare-metal hypervisor from VMware that allows users to virtualize their servers and consolidate applications. The hypervisor has been available since 2008, when it was called Free ESXi 3.5.

The hypervisor lacks some of the enterprise-grade features of the full VMware ESXi version, such as vMotion, Storage vMotion, High Availability, Distributed Resource Scheduler and vSphere Data Protection. However, it does include:

- Thin provisioning of virtual machine disks
- Snapshot and restore capabilities
- Virtual guest operating system support
- Support from the vSphere client
- Hardened device drivers
- Memory over-commitment
- Support for Fibre Channel, iSCSI and NFS shared storage

Users can upgrade to more advanced versions of the VMware vSphere Hypervisor by adding a license file.

ESX runs on bare metal (without running an operating system) unlike other VMware products. It includes its own kernel: A Linux kernel is started first, and is then used to load a variety of specialized virtualization components, including ESX, which is otherwise known as the vmkernel component. The Linux kernel is the primary virtual machine; it is invoked by the service console. At normal run-time, the vmkernel is running on the bare computer, and the Linux-based service console runs as the first virtual machine. VMware dropped development of ESX at version 4.1, and now uses ESXi, which does not include a Linux kernel.

b. KVM hypervisor

KVM hypervisor is the virtualization layer in Kernel-based Virtual Machine (KVM), a free, open source virtualization architecture for Linux distributions.

A hypervisor is a program that allows multiple operating systems to share a single hardware host. In KVM, the Linux kernel acts as a Type 2 Hypervisor, streamlining management and improving performance in virtualized environments. The hypervisor creates virtual machine (VM) environments and coordinates calls for processor, memory, hard disk, network, and other resources through the host OS. KVM requires a processor with hardware virtualization extensions to connect to the guest OS.

KVM has been bundled along with the Linux operating system (OS) since 2007 and can be installed along with the Linux kernel. Numerous guest OSs can work with KVM including BSD (Berkeley Software Distribution), Solaris, Windows, Haiku, ReactOS, Plan 9, and the AROS Research OS. In addition, a modified version of QEMU ("Quick Emulator") can use KVM to run Mac OS X.

By itself, KVM does not perform any emulation. Instead, it exposes the /dev/kvm interface, which a user space host can then use to:

- Set up the guest VM's address space. The host must also supply a firmware image (usually a custom BIOS when emulating PCs) that the guest can use to bootstrap into its main OS.
- Feed the guest simulated I/O.
- Map the guest's video display back onto the system host.

On Linux, QEMU versions 0.10.1 and later is one such user space host. QEMU uses KVM when available to virtualize guests at near-native speeds, but otherwise falls back to software-only emulation.

c. Trust Management

A VMM changes the computer architecture. It provides a layer of software between the operating systems and system hardware to create one or more VMs on a single physical platform. AVM entirely encapsulates the state of the guest operating system running inside it. Encapsulated machine state can be copied and shared over the network and removed like a normal file, which proposes a challenge to VM security. In general, a VMM can provide secure isolation and a VM accesses hardware resources through the control of the VMM, so the VMM is the base of the security of a virtual system. Normally, one VM is taken as a management VM to have some privileges such as creating, suspending, resuming, or deleting a VM.

Once a hacker successfully enters the VMM or management VM, the whole system is in danger.
A subtler problem arises in protocols that rely on the “freshness” of their random number source for generating session keys. Considering a VM, rolling back to a point after a random number has been chosen, but before it has been used, resumes execution; the random number, which must be “fresh” for security purposes, is reused. With a stream cipher, two different plaintexts could be encrypted under the same key stream, which could, in turn, expose both plaintexts if the

plaintexts have sufficient redundancy. Non cryptographic protocols that rely on freshness are also at risk. For example, the reuse of TCP initial sequence numbers can raise TCP hijacking attacks.