**B.E IV/IV Year (IT-A, B) II-SEM, (II-Internal) Examination, March-2016**

**Cloud Computing (Elective-V, BIT-460)**

|  |
| --- |
| CO1: Identify Cloud Security Challenges.  CO2: Identify the need for Common Standards in Cloud Computing. |

[Time: 1 Hour] [Max Marks: 20]

Answer all questions from Part-A

&

Any two questions from Part-B

**Part-A (Mark: 2\*3=6)**

**1. What is virtualization? [CO1] (2M)**

Answer) It means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system.

**2. Explain about federation in cloud? [CO2] (2M)**

Answer) Federation is the ability for two XMPP servers in different domains to exchange XMLstanzas.

1. Permissive federation: Permissive federation occurs when a server accepts a connection from a peer network server without verifying its identity using DNS look-ups or certificate checking.

2. Verified federation: This type of federation occurs when a server accepts a connection from a peer after the identity of the peer has been verified.

3. Encrypted federation: In this mode, a server accepts a connection from a peer if and only if the peer supports Transport Layer Security (TLS) as defined for XMPP

4. Trusted federation: Here, a server accepts a connection from a peer only under the stipulation that the peer supports TLS and the peer can present a digital certificate issued by a root certification authority (CA)

**3. Explain importance of Mobile Internet Devices for the Cloud? [CO2] (2M)**

Answer) The mobile cloud is Internet-based data, applications and related services accessed through smart phones, laptop computers, tablets and other portable devices.

Mobile cloud computing is differentiated from mobile computing in general because the devices run cloud-based [Web apps](http://searchsoftwarequality.techtarget.com/definition/Web-application-Web-app) rather than [native apps](http://searchsoftwarequality.techtarget.com/definition/native-application-native-app). Users subscribe to cloud services and access remotely stored applications and their associated data over the Internet.

Typically, mobile devices run a mix of Web-based and native apps. However, the trend is increasingly toward the mobile cloud. According to ABI Research, the number of mobile cloud computing subscribers is expected to reach 998 million by 2014.

**Part-B (Mark: 2\*7=14)**

**4. Explain about different types of virtualizations. [CO1] (7M)**

|  |  |
| --- | --- |
| **TYPES OF VIRTUALIZATION AND TECHNOLOGIES** | |
| **PARA** | It is simple the **modification of an operating system (usually at the kernel level)** so that it can more closely **resemble its physical machines actual hardware** and it can support only a few operating systems. |
| **FULL** |  |
| **OS** | It refers to the **use of software** to **allow system hardware** to **run multiple instances of different operating systems concurrently**, allowing you to run different applications requiring different operating systems on one computer system. |
| **DENSITY** | It often refers to **the number of virtual machines that can fit within a single physical machine or rack.** The more virtual machines that a single physical machine can support, the more dense it is said to be. |
| **VIRTUALIZATION SOFTWARE** | It is any kind of software that **deals with the emulation of hardware and the splitting up of both physical and software-based resources.**  **Examples**: VMware, Microsoft virtual PC |
| **SOFTWARE VIRTUALIZATION** | ● It is the **virtualization of applications or computer programs.**  ● It involves creating a **virtual layer** or **virtual hard drive space where applications can be installed.**  ● From this virtual space, applications can then be run as though they have been installed onto host OS. |
| **HARDWARE** | Benefit is that the amount of hardware emulation (effort) required is greatly reduced, improving performance. |
| **RESOURCE** | ● It involves the virtualization of one/more IT-related system resources.  ● It could involve the virtualization of specific system resources such as storage or network resources, or it could involve the virtualization of entire physical resources, such as servers or end-user workstations. |
| **PROCESSOR** | It involves the virtualization of a physical processor, so that multiple virtual machines can be run on a single physical machine. |
| **APPLICATION** | ● It works by making separate copies of shared resources for separate applications.  ● For example each virtual application will have a copy of its own drivers, registry entries, DLLs and any other resources that would usually be shared with other applications. |
| **STORAGE** | ● It involves **grouping together multiple physical storage devices** (no matter where they are physically located), so that they appear as one big storage unit. **There are many different storage virtualization technologies including,**  **a. NAS (Network attached Storage)**  A Network-attached storage device is effectively a server that is dedicated to providing file sharing services. It is not concerned with any other services such as e-mail or printer sharing; it only deals with file sharing.  **b. SAN (Storage Area Network)**  It is effectively a sub-network that consists of only storage devices.  ● Storage devices can consist of either a server which contains nothing but hard drives for storage, or a stand-alone rack of storage devices such as a rack of multiple hard drives.  ● ISCSI stands for Internet Small Computer System Interface. SCSI is basically an interface that is used for connecting peripheral devices (including hard drives) to a computer. It acts as a controller, meaning that it doesn’t require software to handle data requests, as it deals with this itself. |
| **DATA STORAGE** | It is used to standardize things, so that end-users did not have to configure anything or keep track of the physical processes of data storage. |
| **INTEL** | ●It is Intel’s hardware assisted virtualization technology.  ● Intel VT technology **utilizes a machine’s hardware-based resources** such as its processor, chipset and BIOS to offload some of its software based virtualization workload to its hardware with near native performance ratios, because virtualization is being carried out directly by hardware, rather than just software alone. |
| **RED HAT** | ● Provides full integration of server and storage virtualization.  ● Provides both para-virtualization and full-virtualization |
| **SOFTGRID APPLICATION** | Same as ALTRIS but from Microsoft |
| **UBUNTU (SERVER EDITION): offers Kernel-based virtual machine (KVM).** | ● KVM is basically Linux’s own full virtualization solution (for example Microsoft Virtual PC is Microsoft’s virtualization solution).  ● KVM can run **multiple virtual machines with a wide range of guest operating systems installed.**  ● It is implemented within the operating systems kernel; it is much more efficient and requires fewer resources than an application-based virtualization solution would.  ● requires far fewer overheads than other application-level virtualization technologies, because it is a part of its operating systems kernel and can communicate directly with the hardware that it is running on. |
| **ALTIRIS** | ● offer virtualization software known as Altiris SVS (Software Virtualization Solution)  ● SVS **allows you to install software applications** on to your machine but in a virtualized area.  ● This means that applications are not actually installed on to your physical machine, instead they reside in a virtual location. This virtual location can then be activated or deactivated at will. |

**5. Explain Cloud security challenges. [CO1] (7M)**

-Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm. This is particularly true for the SaaS provider.

-With the cloud model, you lose control over physical security. In a public cloud, you aresharing computing resources with other companies.

-Storage services provided by one cloud vendor may be incompatible with another vendor’s services should you decide to move from one to the Other.

-If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Is it the customer or the cloud vendor?

-Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval). Put simply, data integrity is assurance that the data is consistent and correct.

-The immature use of mash up technology (combinations of web services), which is fundamental to cloud applications, is inevitably going to cause unwitting security vulnerabilities in those applications. Your development tool of choice should have a security model embedded in it to guide developers during the development phase and restrict users only to their authorized data when the system is deployed into production.

-As more and more mission-critical processes are moved to the cloud, SaaS suppliers will have to provide log data in a real-time, straightforward manner, probably for theiradministrators as well as their customers’ personnel.

-Cloud applications undergo constant feature additions, and users must keep up to datewith application improvements to be sure they are protected.

-Having proper fail-over technology is a component of securing the cloud that is often over looked. The company can survive if a non-mission critical application goes offline,

but this may not be true for mission-critical applications.

-Outsourcing means losing significant control over data, and while this isn’t a good idea from a security perspective, the business ease and financial savings will continue to increase the usage of these services. Security managers will need to work with their company’s legal staff to ensure that appropriate contract terms are in place to protect corporate data and provide for acceptable service-level agreements.

-Cloud-based services will result in many mobile IT users accessing business data and services without traversing the corporate network. This will increase the need for enterprises to place security controls between mobile users and cloud-based services.

-Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co-located on the same physical resources. Although traditional datacenter security still applies in the cloud environment, physical segregation and hardware based security cannot protect against attacks between virtual machines on the same server.

-Operating system and application files are on a shared physical infrastructure in a virtualized cloud environment and require system, file, and activity monitoring to provide confidence and auditable proof to enterprise customers that their resources have not been compromised or tampered With

-To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself.

**6. Explain about Common Standards in Cloud Computing. [CO2] (7M)**

**Common Standards in Cloud Computing**

1 Chapter Overview

2 The Open Cloud Consortium

3 The Distributed Management Task Force

3.1 Open Virtualization Format

4 Standards for Application Developers

4.1 Browsers (Ajax)

4.2 Data (XML, JSON)

4.3 Solution Stacks (LAMP and LAPP)

5 Standards for Messaging

5.1 Simple Message Transfer Protocol (SMTP)

5.2 Post Office Protocol (POP)

5.3 Internet Messaging Access Protocol (IMAP)

5.4 Syndication (Atom, Atom Publishing Protocol, and RSS)

5.5 Communications (HTTP, SIMPLE, and XMPP)

6 Standards for Security

6.1 Security (SAML OAuth, OpenID, SSL/TLS)