Internal Assessment Test 2 –November 2024

Sub:	Cloud Computing			Sub Code:	21CS72	Branch:		AInDS	
Date:		Duration:	90 min	Max Marks:	50	Sem:	VII	OBE	
Answer any FIVE Questions							**MARKS**	**CO**	**RBT**
Q1.	What are the fundamental concepts introduced in the cloud reference architecture? What kinds of needs are addressed by heterogeneous clouds?						5+5	CO3	L4
Q2.	What are the basic components of an IAAS based solution for cloud computing? Classify the various types of clouds.						5+5	CO3	L3
Q3.	What are the main characteristics of a Platform-as-a-Service solution, Infrastructure -as-a-service and Software-as-a-Service solutions? What are the fundamental features of the economic and business model behind cloud computing?						6+4	CO3	L4
Q4.	What are the cloud security risks? Draw a diagram to show the attacks in cloud computing.						10	CO4	L4
Q5.	What are the key security risks associated with virtual machines? Explain with a diagram.						10	CO4	L3
Q6.	What role does the management operating system (Dom0) play in the Trusted Computing Base (TCB) of a Xen environment, and how does it contribute to system vulnerabilities according to the analysis of Xen attacks? Provide a diagram.						10	CO4	L3

Answers

1. Cloud computing architecture consists of the frontend, backend, service models, deployment models, networking, virtualization, and management tools. The frontend includes user interfaces on client devices, while the backend provides cloud infrastructure (storage, compute resources, security) and application services accessed through networks like the internet. Services are categorized into models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), with deployment options like public, private, and hybrid clouds.

Cloud infrastructure is heterogeneous, utilizing various resources like clusters and networked PCs, along with database systems and storage services. The core middleware manages the physical infrastructure to provide an optimal runtime environment for applications and efficient resource utilization. At the foundational level, virtualization technologies ensure customization, isolation, sandboxing, and quality of service. Hypervisors ensure resource management and present the distributed infrastructure as virtual machines, allowing for precise partitioning of hardware resources like CPU and memory to meet user and application needs. This solution is often combined with storage and network virtualization to enable complete control over the infrastructure.

2. Infrastructure as a Service (IaaS) is a business model that delivers IT infrastructure like compute, storage, and network resources on a pay-as-you-go basis over the internet. We can use IaaS to request and configure the resources we require to run our applications and IT systems. We are responsible for deploying, maintaining, and supporting our applications, and the IaaS provider is responsible for maintaining the physical infrastructure.

Infrastructure as a Service.

TYPES OF CLOUDS

Cloud computing comes in several types, mainly based on deployment models and the way resources are shared. The primary types of cloud are:

Public Cloud

Public clouds represent the foundational model of cloud computing, providing services accessible to anyone, from anywhere, at any time via the Internet. A core feature of public clouds is multitenancy, where numerous customers share the same infrastructure but operate within isolated virtual environments, ensuring performance and quality of service (QoS).

Private Cloud

Private clouds are cloud infrastructures dedicated to a single organization, providing all the benefits of cloud computing—such as scalability, flexibility, and resource efficiency—while maintaining full control over data and IT infrastructure. In a private cloud, resources can be dynamically allocated to departments or teams as needed, often through internal billing or resource tracking systems.

Hybrid Cloud

Hybrid clouds combine elements of both public and private clouds, allowing organizations to manage workloads across both environments for optimal flexibility, security, and scalability. This model allows IT teams to optimize resource use, reduce operational costs, and ensure data sovereignty while meeting complex security and compliance needs.

Community Cloud

Community clouds are a cloud infrastructure model designed for use by a specific group of organizations that have similar needs, such as shared regulatory, compliance, security, or mission requirements. In a community cloud, resources are jointly owned, managed, and operated either by the participating organizations themselves or by a third-party provider. This infrastructure allows organizations to benefit from the advantages of cloud computing like scalability, flexibility, and cost savings.

3. Platform as a Service (PaaS):

- PaaS provides a platform that includes tools, libraries, and frameworks, enabling developers to build, test, and deploy applications without managing underlying hardware or operating systems.
- Automatically scales resources based on application demand.
- Offers built-in tools for database management, development, and analytics, making it easier to build applications quickly.
- The cloud provider handles maintenance, upgrades, and security of the infrastructure.

Infrastructure as a Service (IaaS):

- Provides virtualized computing resources, such as servers, storage, and networking, enabling users to configure their own environment.
- Users have control over operating systems, applications, and configurations.

- Easily scales up or down based on demand.
- Users only pay for the resources they use, which reduces the need for physical hardware investments.

Software as a Service (SaaS):

- Delivers applications over the internet, managed and maintained by the provider.
- Users can access the software from any device with internet access, typically through a web browser.

The main drivers of cloud computing are economy of scale and simplicity of software delivery and its operation. In fact, the biggest benefit of this phenomenon is financial:

• the pay-as-you-go model offered by cloud providers. In particular, cloud computing allows:
• Reducing the capital costs associated to the IT infrastructure
• Eliminating the depreciation or lifetime costs associated with IT capital assets
• Replacing software licensing with subscriptions
• Cutting the maintenance and administrative costs of IT resources.

Capital costs are one-time expenses for essential assets like IT infrastructure and software that support long-term business operations. Common to all businesses, these costs reduce over time as hardware loses value and software ages, impacting profits. Keeping capital costs low is advantageous, as it reduces long-term expenses associated with asset depreciation and replacement needs. The amount of cost savings that cloud computing can introduce within an enterprise is related to the specific scenario in which cloud services are used and how they contribute to generate a profit for the enterprise.

4. Traditional Threats in Cloud Security

These are security risks that have existed in IT environments long before the cloud, but they still apply in the cloud context due to the nature of cloud services. These include:

- Malware: Malicious software such as viruses, ransomware, and spyware can still affect cloud-based applications and data. Cloud systems may be targeted by malware through user devices or in the cloud infrastructure.

- Phishing: Cloud users are still vulnerable to phishing attacks.

- Denial of Service (DoS): While cloud environments have built-in protections, DoS and Distributed Denial of Service (DDoS) attacks can still affect the availability of cloud services. Cloud services are often targeted by attackers who aim to overwhelm resources and disrupt service.

Availability of Cloud Services: Availability risks are crucial because cloud systems are often mission-critical, and downtime can have significant operational and financial impacts. Common availability risks in cloud environments include:

- Service Outages: Cloud providers may experience outages due to hardware failures, network issues, or system misconfigurations.

- Over-reliance on a Single Cloud Provider: If a business heavily depends on one cloud provider for critical services, any service interruptions could cause significant disruption.

Third-Party Control: One of the most significant aspects of cloud computing is that users are outsourcing their infrastructure, platform, or software to a third-party cloud provider. This introduces several risks:

- Lack of Visibility and Control: Customers may not have full visibility into the cloud provider's security practices, infrastructure, and data handling procedures. This makes it challenging to assess security risks effectively customized security measures.

- Third-Party Service Providers: Many cloud environments integrate with external third-party services (e.g., APIs, SaaS applications). These services may introduce additional risks, as they may not be as secure as the main cloud provider.

Data Loss or Leakage: Data stored in the cloud can be lost, exposed, or compromised due to various factors, such as poor management practices, security breaches, or even natural disasters:

- Accidental Deletion: Cloud users might accidentally delete or overwrite critical data. Without proper data backup and recovery mechanisms in place, the data could be permanently lost.

- Misconfigurations: Incorrectly configured cloud storage settings (e.g., public access settings for storage volumes) can lead to unintentional exposure of sensitive data. This is a common cause of data leakage in cloud environments.

- Data In Transit Risks: If encryption protocols are not used for data in transit (when data moves between the user and the cloud or between different cloud services), attackers can intercept and compromise sensitive data.

- Data Breaches: Cloud services may be targeted by hackers looking to access large datasets. If vulnerabilities exist in the cloud provider's infrastructure, an attacker may exploit them to access private information.

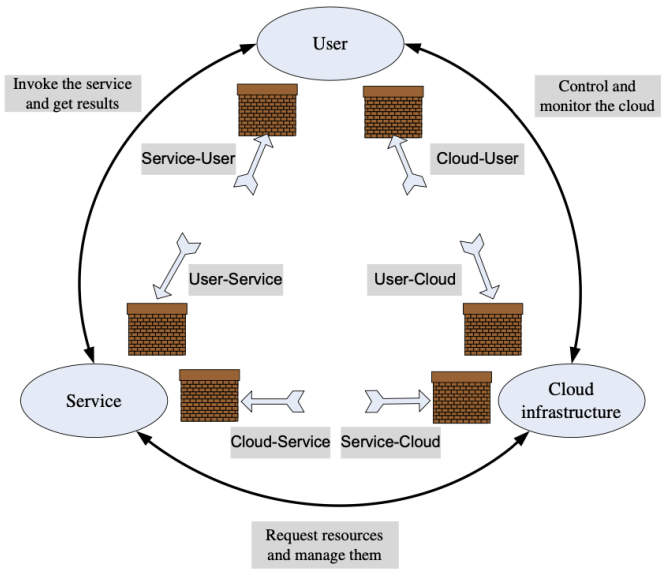
Account or Service Hijacking: Cloud accounts and services can be hijacked in several ways, typically through weaknesses in user authentication or the misuse of privileged access. These include:

- Credential Theft: If attackers gain access to user credentials (via phishing, social engineering, or breaches in other systems), they can hijack cloud accounts and perform malicious actions such as accessing, modifying, or deleting sensitive data.

- Privilege Escalation: Attackers who gain access to lower-level accounts (e.g., through weak passwords or misconfigurations) might exploit vulnerabilities to escalate privileges and gain administrator-level access to cloud services.

- Compromised API Keys: Cloud services often use API keys for programmatic access. If these keys are exposed or stolen, attackers can perform actions on behalf of the account holder, including data manipulation, resource provisioning, or service disruption.

- Service Hijacking: In some cases, attackers can hijack an organization's cloud services to launch malicious campaigns, such as cryptocurrency mining or phishing campaigns, using the resources provided by the cloud platform.



5. Virtual machine (VM) security focuses on the traditional system VM model where a Virtual Machine Monitor (VMM) controls hardware access, ensuring stricter isolation than traditional operating systems. The VMM provides or enables security services, such as memory and resource isolation, and facilitates cloning, replication, and encryption of VMs to enhance security and reliability.
Challenges include limited visibility of high-level operations, the risk of compromised trusted computing bases (TCBs), and potential exploitation of VM fingerprinting or log file access by attackers. Security enhancements come at a cost, including higher hardware requirements, development efforts, and performance overhead.

VMM-Based Threats:

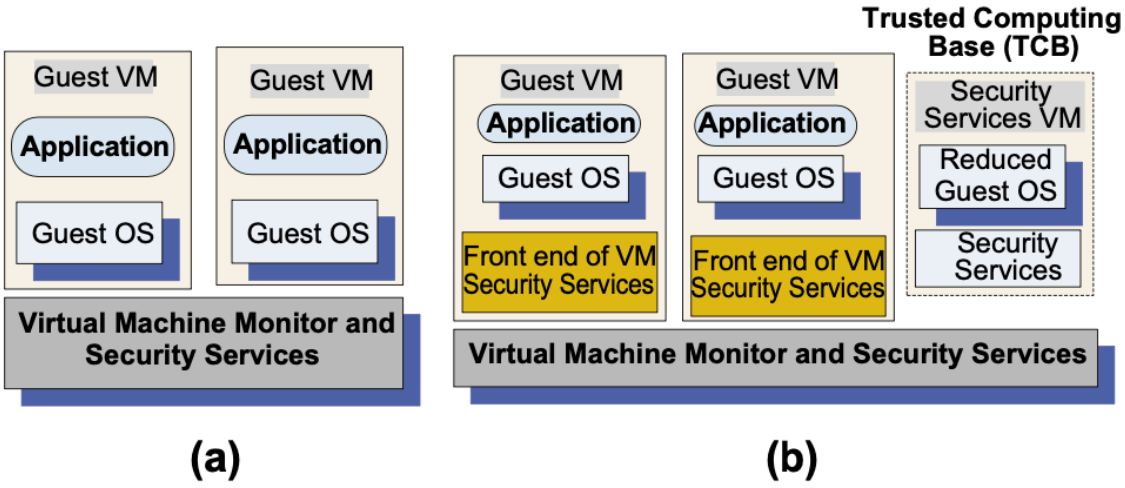
1. Resource Starvation and Denial of Service: Misconfigured resource limits or rogue VMs bypassing limits can disrupt resource allocation.
2. VM Side-Channel Attacks: Rogue VMs exploit weaknesses in inter-VM traffic isolation, insufficient packet inspection for high-speed traffic, or insecure VM images lacking updates.
3. Buffer Overflow Attacks: Exploitation of software vulnerabilities in the VMM.

VM-Based Threats:

1. Rogue or Insecure VM Deployment: Unauthorized actions like creating or modifying VMs stem from poorly configured access controls.
2. Tampered or Insecure VM Images: Lack of repository access controls and image integrity verification, such as digital signatures, allows compromised VM images.

6. While virtualization enhances security through stronger VM isolation and smaller hypervisor codebases (e.g., Xen's ~60,000 lines of code), it introduces risks through the management OS (e.g., Dom0 in Xen environments). The management OS plays a critical role in VM creation, data transfer, and device management, becoming part of the Trusted Computing Base (TCB). Key risks include:

1. Expanded Attack Surface:



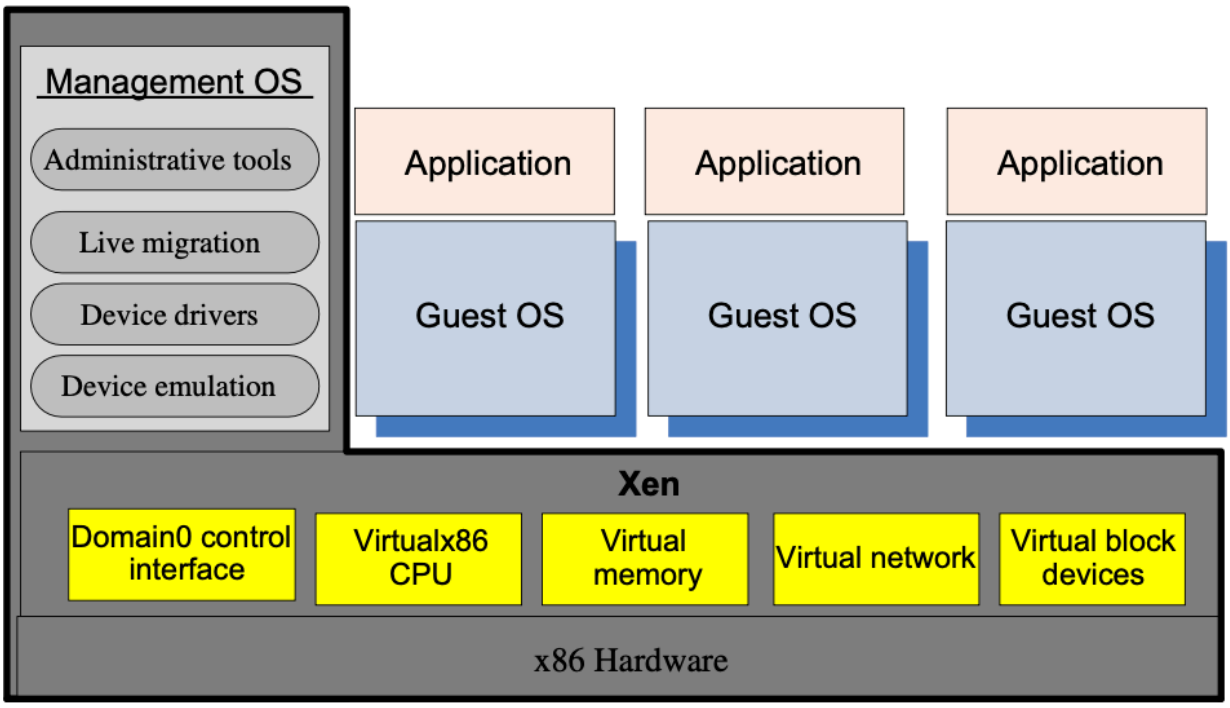
- The TCB includes both the hypervisor and the management OS, increasing potential vulnerabilities.
- Most attacks target the control VM (Dom0), including buffer overflows, denial-of-service (DoS), and memory access exploits.

2. Dom0-Specific Weaknesses:
   - Dom0 manages system state via XenStore, making it a critical vulnerability point for DoS and unauthorized memory access by malicious VMs.
   - Cryptographic keys stored in DomU memory can potentially be extracted by Dom0, even with TLS encryption.
3. Memory Sharing Risks:
   - Foreign mapping by Dom0 enables unauthorized access to DomU memory.
   - Security improvements require restricting memory sharing to hypervisor-monitored, encrypted exchanges initiated by DomU.

Mitigation Strategies

- Restrict Dom0 Privileges: Limit Dom0's ability to perform foreign mapping and ensure that memory sharing is initiated securely by DomU.
- Encryption and Integrity Checks: Use encrypted memory pages and virtual CPU registers during interactions, with hypervisor monitoring for integrity validation.
- Harden XenStore: Enhance access controls to prevent malicious VMs from exploiting XenStore.

Addressing these risks ensures stronger isolation and maintains the integrity and confidentiality of virtualized environments.


Management OS
Administrative tools
Live migration
Device drivers
Device emulation
Application
Application
Application
Guest OS
Guest OS
Guest OS
Xen
Domain0 control interface
Virtualx86 CPU
Virtual memory
Virtual network
Virtual block devices
x86 Hardware