CMR INSTITUTE OF TECHNOLOGY

USN :____________________ CMRIT

Internal Assessment Test 3

Sub:	**Cloud Computing**	**Subject Code:**	**21CS72**	**Branch :**	**AI & DS**
Date:		**Duration: 90 min**	**Marks : 50**	**Sem : VII**	**OBE**

Answer any FIVE question	**Marks**	**CO**	**RBT**
1. How can operating system security mechanisms be improved to better protect applications from malicious attacks?	10	CO3	L2
2. What are the primary security challenges associated with virtual machines in a cloud environment?	10	CO3	L2
3. What security risks are introduced by a management operating system in virtualization?	10	CO4	L3
4. What is AWS? What are the 6 major configuration for EC2 instances?	10	CO4	L3
5. Describe an application of cloud computing technology in the field of biology.	10	CO4	L2
6. Describe how cloud computing technology can be applied to support remote ECG monitoring.	10	CO4	L3

CI CCI HOD

ANSWERS

1 ans.

Operating system (OS) security is crucial for protecting applications from various malicious attacks, including unauthorized access and code tampering. An OS facilitates resource sharing among applications while enforcing security policies to mitigate risks, even on single-user devices like PCs and smartphones. Mandatory security policies, defined and controlled by a system security administrator, encompass access control, authentication, and cryptographic mechanisms. Trusted applications—those that perform security functions— should operate with minimal privileges to enhance security. To improve security, complex mechanisms can be decomposed into defined components, such as separating access control into enforcer and decider roles. This structure ensures that access to protected resources is carefully managed based on established security policies. Specialized closed-box platforms, like certain cell phones and ATMs, can use embedded cryptographic keys for secure identity verification and software authentication, a feature not found in open-box platforms with commodity operating systems. While a secure operating system is essential, application-specific security is often more effective, especially in contexts like electronic commerce that require digital signatures.

2 ans.

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:

Resource Starvation and Denial of Service: Misconfigured resource limits or rogue VMs bypassing limits can disrupt resource allocation.

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.

Buffer Overflow Attacks: Exploitation of software vulnerabilities in the VMM.

VM-Based Threats:

Rogue or Insecure VM Deployment: Unauthorized actions like creating or modifying VMs stem from poorly configured access controls.

Tampered or Insecure VM Images: Lack of repository access controls and image integrity verification, such as digital signatures, allows compromised VM images.

3 ans.

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.

4 ans.

Amazon Web Services (AWS) provides a broad range of cloud computing services that cater to various needs of businesses and developers. Below are detailed explanations of its key service categories: compute, storage, communication, and additional services.

1. <u>Compute Services:</u>

AWS compute services provide the foundational resources to run applications, process data, and perform computational tasks.

Key Compute Services:

Amazon EC2 (Elastic Compute Cloud):

Available configurations for EC2 instances. There are six major categories (features):

- Standard instances. This class offers a set of configurations that are suitable for most applications. EC2 provides three different categories of increasing computing power, storage, and memory.
- Micro instances. This class is suitable for those applications that consume a limited amount of computing power and memory and occasionally need bursts in CPU cycles to process surges in the workload. Micro instances can be used for small Web applications with limited traffic.
- High-memory instances. This class targets applications that need to process huge workloads and require large amounts of memory. Three-tier Web applications characterized by high traffic are the target profile. Three categories of increasing memory and CPU are available, with memory proportionally larger than computing power.
- High-CPU instances. This class targets compute-intensive applications. Two configurations are available where computing power proportionally increases more than memory.
- Cluster Compute instances. This class is used to provide virtual cluster services. Instances in this category are characterized by high CPU compute power and large memory and an extremely high I/O and network performance, which makes it suitable for HPC applications.
- Cluster GPU instances. This class provides instances featuring graphic processing units (GPUs) and high compute power, large memory, and extremely high I/O and network performance. This class is particularly suited for cluster applications that perform heavy graphic computations, such as rendering clusters. Since GPU can be used for general-purpose computing, users of such instances can benefit from additional computing power, which makes this class suitable for HPC applications.

5 ans.

Biology: Gene Expression Data Analysis for Cancer Diagnosis on Cloud Computing

Cloud computing offers an advanced solution for gene expression data analysis, which plays a crucial role in cancer diagnosis and personalized treatment. By analyzing gene expression data from cancer cells, researchers and healthcare providers can identify molecular patterns and biomarkers that indicate the presence of cancer and determine its subtype, aiding in more accurate and timely diagnoses.

Key benefits of using cloud computing for gene expression data analysis in cancer diagnosis:

1. Scalability: Cloud platforms provide scalable resources to handle vast amounts of gene expression data from large cohorts of cancer patients. This allows researchers and clinicians to analyze and process data without limitations on computational power or storage capacity.
2. Advanced Analytics: Cloud computing enables the application of machine learning, deep learning, and other advanced algorithms to identify cancer-related genetic markers and predict disease progression, enabling more accurate diagnoses and targeted treatments.
3. Collaboration: Cloud-based platforms allow multiple research teams and clinicians to collaborate across geographies, sharing insights, datasets, and findings in real-time, enhancing the understanding of cancer genomics.
4. Cost Efficiency: Instead of investing in expensive on-premises infrastructure, healthcare organizations can leverage cloud resources on a pay-per-use basis, reducing the financial burden on cancer research and diagnostic labs.

5. Data Security: Cloud service providers offer robust security measures such as encryption, access control, and compliance with healthcare regulations (like HIPAA) to protect sensitive genetic data and ensure patient privacy.
6. Integration with Other Data Sources: Cloud computing can integrate gene expression data with clinical and imaging data, providing a comprehensive approach to cancer diagnosis and treatment planning.

6 ans.

Healthcare: ECG Analysis in the Cloud

ECG (Electrocardiogram) analysis in the cloud involves using cloud-based platforms to process, store, and analyze ECG data. With the integration of cloud computing, healthcare providers can access ECG data remotely, enabling real-time monitoring, diagnosis, and long-term tracking of patients' heart health.

Key benefits of cloud-based ECG analysis include:

1. Remote Monitoring: Patients can have their ECGs recorded through portable devices, and the data is sent to the cloud for analysis, allowing doctors to monitor heart health from anywhere.
2. Scalability: Cloud platforms can handle large amounts of ECG data, enabling hospitals and clinics to scale their ECG monitoring services without investing heavily in infrastructure.
3. Advanced Analytics: Cloud computing can leverage machine learning algorithms to detect irregularities, such as arrhythmias, in ECG patterns, providing accurate diagnostics and improving treatment outcomes.
4. Collaboration: Healthcare professionals across the world can access and collaborate on ECG data, improving second-opinion consultations and diagnosis accuracy.
5. Data Security: Cloud providers offer encryption and secure access protocols to ensure that sensitive patient data is protected while being stored and transmitted.