Cloude Computing

Module -4

- **Resource Monitoring Techniques**

Resource monitoring in cloud computing involves managing and controlling how capabilities provided by cloud resources and services are made available to other entities, such as users, applications, or services.
Compute Model: This model allows all users to share resources in the cloud at the same time. It enables users to reserve the VM's memory to ensure that the memory size requested by the VM is always available to operate locally on clouds with a good enough level of QoS (Quality of Service) being delivered to the end user.
Data Model: This model is related to plotting, separating, querying, transferring, caching, and replicating data.
Virtualization: This method creates an emulation of software or hardware on our computer. It has two components: Abstraction, which provides the necessary virtual versions of raw compute, storage, and network that can be unified as a pool of resources and resource overlay which includes data storage services, and a web hosting environment; and Encapsulation, where a virtual machine can be represented as a single file.

- **How to access compute (windows and Linux) from internet? describe tools and its security**

Accessing a compute resource remotely over the internet can be achieved using different tools and methods.

Windows:
Remote Desktop Protocol (RDP): Windows has a built-in tool called Remote Desktop, which uses the Remote Desktop Protocol (RDP) to connect to another computer over the internet.
Virtual Private Network (VPN): A VPN can be used to create a secure connection to the network where the compute resource is located.
Third-Party Tools: There are several third-party tools available such as TeamViewer and Chrome Remote Desktop that allow you to access your computer remotely.

Linux:
Secure Shell (SSH): SSH is a protocol that allows you to connect and authenticate to remote servers and services. With SSH, you can manage machines, copy files, and more.
Virtual Network Computing (VNC): VNC allows you to remotely access a graphical desktop environment. To use VNC, you need to install a VNC server on the machine you want to access.
Third-Party Tools: Similar to Windows, you can use third-party tools like TeamViewer and Chrome Remote Desktop for remote access.

Security Measures: When accessing compute resources over the internet, it's crucial to consider security measures to protect your data and systems.
Use Secure Connections: Always use a secure connection when connecting to the internet. If you're using a public network, consider using a secure Virtual Private Network (VPN).
Strong Passwords: Select strong passwords that are harder for cybercriminals to crack. A strong password is long, includes a mix of characters, and avoids obvious sequences or personal information.
Firewalls: Firewalls can prevent unauthorized access to your network and computer systems.
Regular Backups: Regularly backing up your data helps mitigate the impact of a ransomware attack.
Software Updates: Keep your operating system and all software, including your remote access tools, up to date to protect against known vulnerabilities.

- **Encryption Technologies and Methods**

Encryption is a crucial technology in cloud computing, used to protect data from being stolen, changed, or compromised. It works by scrambling data into a secret code that can only be unlocked with a unique digital key.

Encryption Technologies:
Symmetric Encryption: This method uses the same key for both encryption and decryption. It's less expensive to produce and doesn't require as much computing power to encrypt and decrypt, meaning there's less delay in decoding the data.
Asymmetric Encryption: Also known as public key encryption, this method uses two different keys - a public key for encryption and a private key for decryption.
Hash Functions: These create a unique digest of a message to ensure its integrity.

Encryption Methods:
Data Encryption Standard (DES): This is a symmetric-key algorithm that's used widely in cryptography.
Advanced Encryption Standard (AES): This is a more secure symmetric encryption algorithm and is used extensively across many security systems.
Identity Based Encryption (IBE): This is a type of public key encryption that allows a third-party server to generate keys based on the recipient's identity.
Rivest, Shamir, Adleman, Algorithm (RSA): This is one of the first public-key cryptosystems and is widely used for secure data transmission.

- **Describe network security in cloud, compute security and storage security**

Network Security in Cloud Computing: Network security in cloud computing involves implementing security measures to protect cloud-based infrastructure. This includes the use of technologies such as SSL (Secure Socket Layer) Encryption, Multi Tenancy based Access Control, Intrusion Detection Systems, firewalls, penetration testing, tokenization, and VPN (Virtual Private Networks). It also involves avoiding public internet connections and using secure connections for data transmission.

Compute Security in Cloud Computing: Compute security in cloud computing refers to the protection of cloud environments, data, information, and applications against unauthorized access, DDOS attacks, malwares, hackers, and other similar attacks. This involves implementing security techniques such as SSL Encryption, Multi Tenancy based Access Control, Intrusion Detection System, firewalls, penetration testing, tokenization, VPNs, and avoiding public internet connections.

Storage Security in Cloud Computing: Storage security in cloud computing involves protecting data stored in the cloud from leakage, theft, and data loss. This includes encrypting data, continuously monitoring data to protect against cybersecurity threats, and storing data redundantly to ensure that a copy will survive any catastrophe. It also involves implementing physical security, technology tools, access management and controls, and organizational policies.