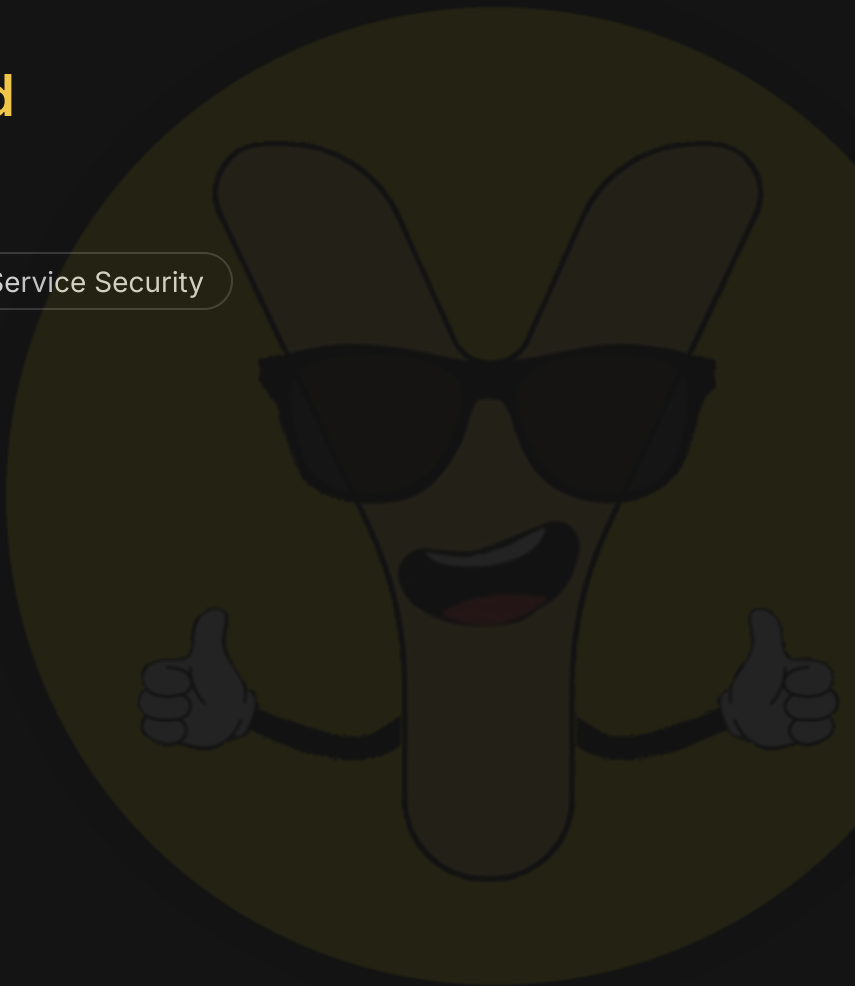
AKTU · 4TH YEAR · SEMESTER 7 · BCS071

Cloud Computing

Unit 4 — Resource Management And Security In Cloud

- Inter Cloud Resource Management
- Resource Provisioning and Resource Provisioning Methods
- Global Exchange of Cloud Resources
- Security Overview
- Cloud Security Challenges
- Software-as-a-Service Security
- Security Governance
- Virtual Machine Security
- IAM
- Security Standards



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Inter-Cloud Resource Management

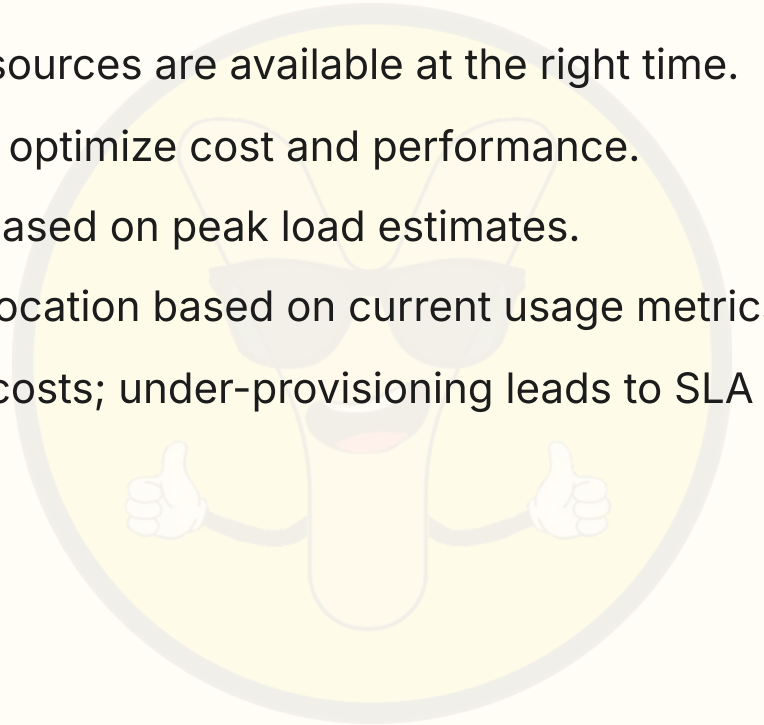
Inter-cloud resource management involves coordinating resources across multiple heterogeneous cloud service providers.

- Enables seamless workload migration between different cloud environments.
- Facilitates resource sharing to handle peak demands (Cloud Bursting).
- Prevents vendor lock-in by allowing interoperability.
- Requires standardized APIs and protocols for communication.
- Challenges include latency, data consistency, and security synchronization.

Resource Provisioning

Resource provisioning is the process of allocating cloud resources to applications based on demand.

- Ensures that the right amount of resources are available at the right time.
- Goal: Match supply with demand to optimize cost and performance.
- Static Provisioning: Pre-allocation based on peak load estimates.
- Dynamic Provisioning: Real-time allocation based on current usage metrics.
- Over-provisioning leads to wasted costs; under-provisioning leads to SLA violations.

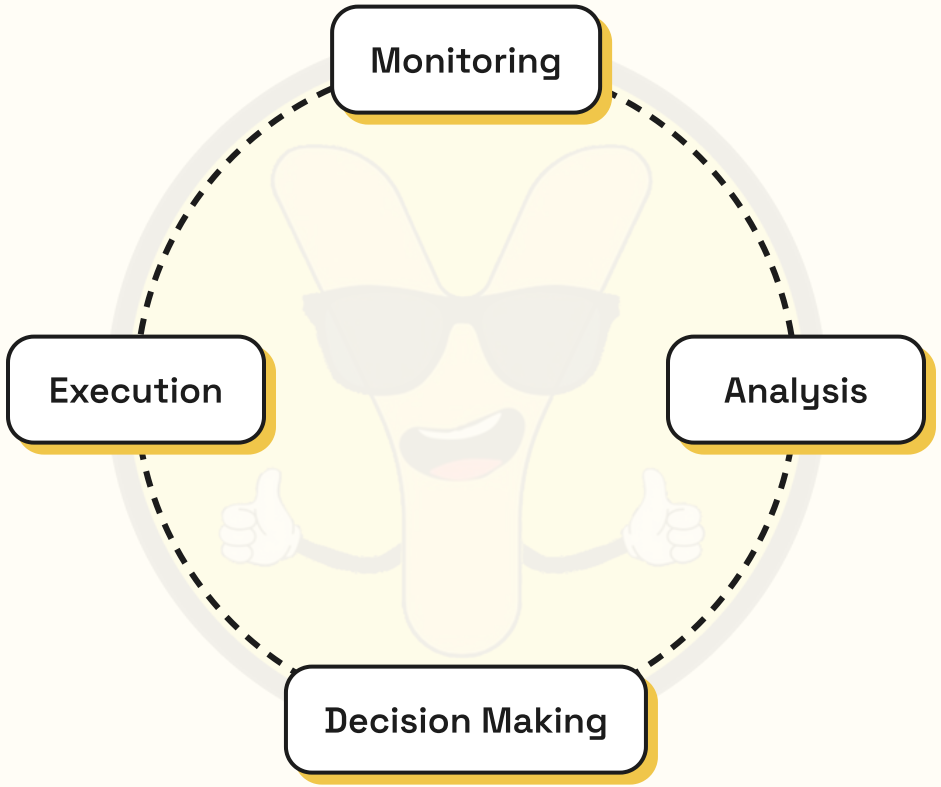


Resource Provisioning Methods

Various strategies are used to manage the lifecycle of cloud resources.

- Reactive Provisioning: Triggers allocation when thresholds (e.g., CPU > 80%) are hit.
- Proactive Provisioning: Uses historical data and predictive models to anticipate future needs.
- Market-based Provisioning: Resources are allocated based on auctions or bidding.
- Lease-based Provisioning: Resources are acquired for a fixed time duration.
- Policy-based Provisioning: Automated rules define allocation based on business constraints.

Resource Provisioning Cycle



The continuous loop of managing cloud resource allocation.

Global Exchange of Cloud Resources

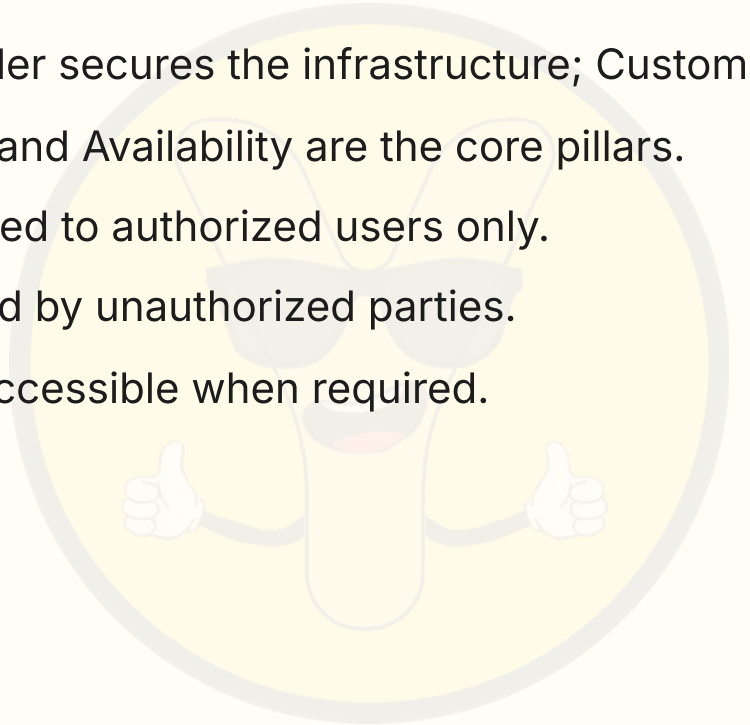
Cloud resource exchange allows providers to trade idle capacity.

- Cloud Brokerage: Acts as an intermediary between users and multiple providers.
- Cloud Federation: Multiple clouds cooperate to share resources under a common policy.
- Resource Trading: Allows buying/selling of computing power via a marketplace.
- Benefits: Improved resource utilization and reduced operational costs.
- Requirements: Standardized accounting, billing, and resource discovery mechanisms.

Cloud Security Overview

Security in the cloud is a shared responsibility between the provider and the customer.

- Shared Responsibility Model: Provider secures the infrastructure; Customer secures data and applications.
- CIA Triad: Confidentiality, Integrity, and Availability are the core pillars.
- Confidentiality: Data access restricted to authorized users only.
- Integrity: Ensuring data is not altered by unauthorized parties.
- Availability: Ensuring services are accessible when required.



Cloud Security Challenges

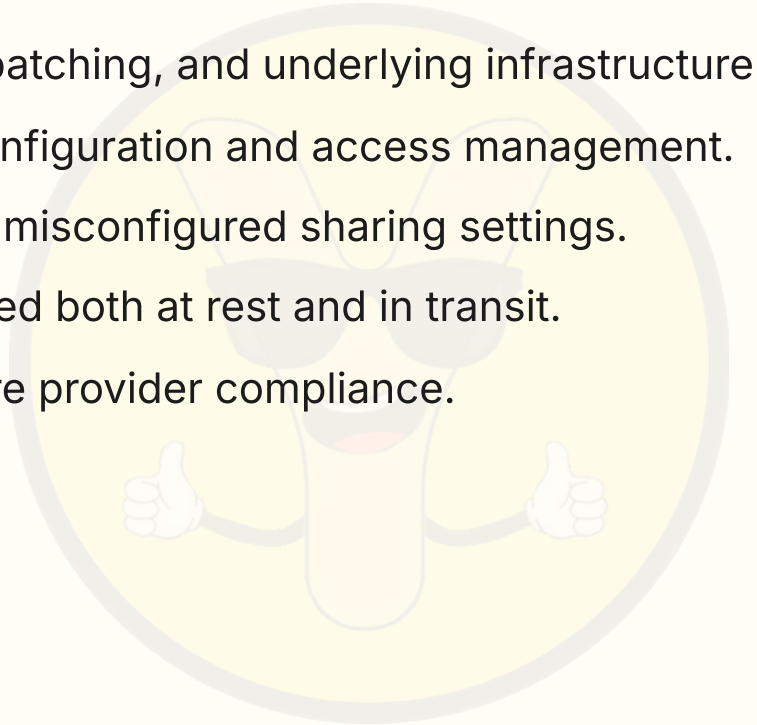
Cloud environments introduce unique security vulnerabilities compared to on-premise systems.

- Data Breaches: Unauthorized access to sensitive information.
- Insecure APIs: Weak interfaces can lead to system compromise.
- Account Hijacking: Attackers gaining control of user credentials.
- Insider Threats: Malicious or negligent actions by internal employees.
- Multi-tenancy Risks: Potential for side-channel attacks between tenants.

SaaS Security

Software-as-a-Service security focuses on application-level protection.

- Provider manages the application, patching, and underlying infrastructure.
- Customer is responsible for data configuration and access management.
- Key concern: Data leakage through misconfigured sharing settings.
- Encryption: Data should be encrypted both at rest and in transit.
- Regular audits are required to ensure provider compliance.



Security Governance

Governance provides the framework for managing security risks effectively.

- Defines policies, procedures, and standards for cloud usage.
- Ensures alignment between IT security and business objectives.
- Compliance: Adherence to legal and regulatory requirements (e.g., GDPR, HIPAA).
- Risk Management: Identifying, assessing, and mitigating cloud-related threats.
- Accountability: Clearly defined roles and responsibilities for security tasks.



Virtual Machine Security

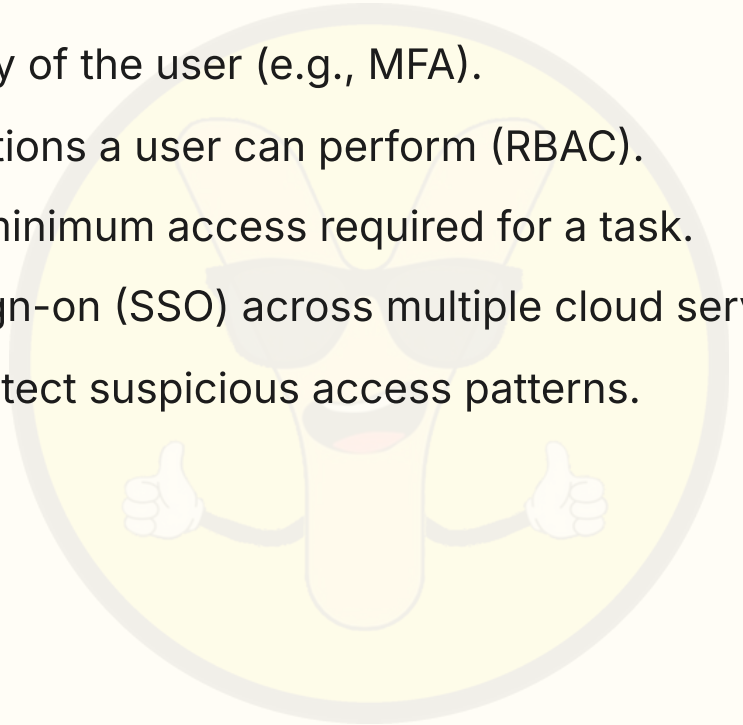
Securing the virtualization layer is critical to prevent cross-VM attacks.

- Hypervisor Hardening: Protecting the software that manages virtual machines.
- VM Isolation: Ensuring one VM cannot access memory or storage of another.
- Snapshot Security: Protecting VM images from unauthorized access.
- Patch Management: Regularly updating guest OS and applications within VMs.
- Network Segmentation: Using virtual firewalls to isolate VM traffic.

Identity and Access Management (IAM)

IAM ensures that only authorized users access specific cloud resources.

- Authentication: Verifying the identity of the user (e.g., MFA).
- Authorization: Determining what actions a user can perform (RBAC).
- Least Privilege Principle: Granting minimum access required for a task.
- Centralized Management: Single sign-on (SSO) across multiple cloud services.
- Monitoring: Auditing user logs to detect suspicious access patterns.



Security Standards

Adherence to standards builds trust and ensures interoperability.

- ISO/IEC 27017: Code of practice for cloud service information security.
- ISO/IEC 27018: Protection of personal data in the cloud.
- SOC 2: Reports on controls at a service organization relevant to security.
- PCI DSS: Standards for handling credit card information.
- NIST Cloud Computing Security Reference Architecture.



Exam corner

- **Q1** Explain the difference between static and dynamic resource provisioning.
- **Q2** Describe the Shared Responsibility Model in cloud security.
- **Q3** What are the major security challenges in a multi-tenant cloud environment?
- **Q4** Explain the role of IAM in cloud security with an example.
- **Q5** Discuss the significance of ISO/IEC 27017 in cloud governance.
- **Q6** How can hypervisor vulnerabilities impact virtual machine security?
- **Q7** Differentiate between reactive and proactive resource provisioning methods.

Unit 4 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 5 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

