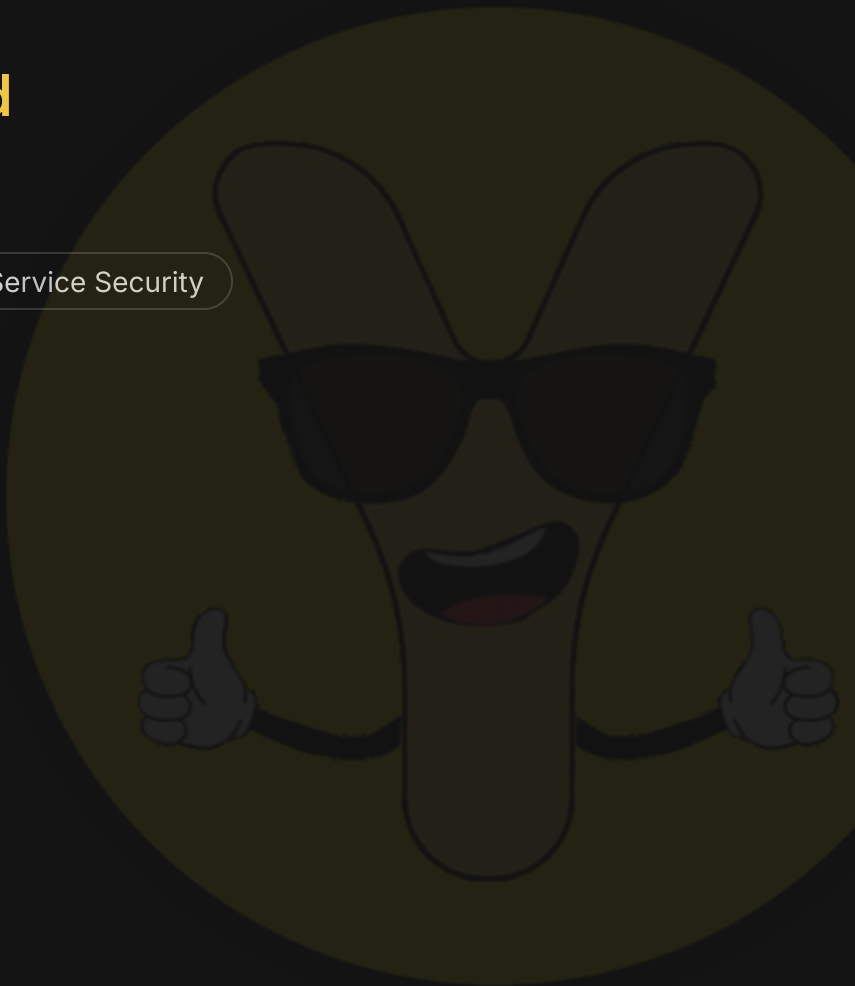
AKTU · 3RD YEAR · SEMESTER 5 · BCAM051

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

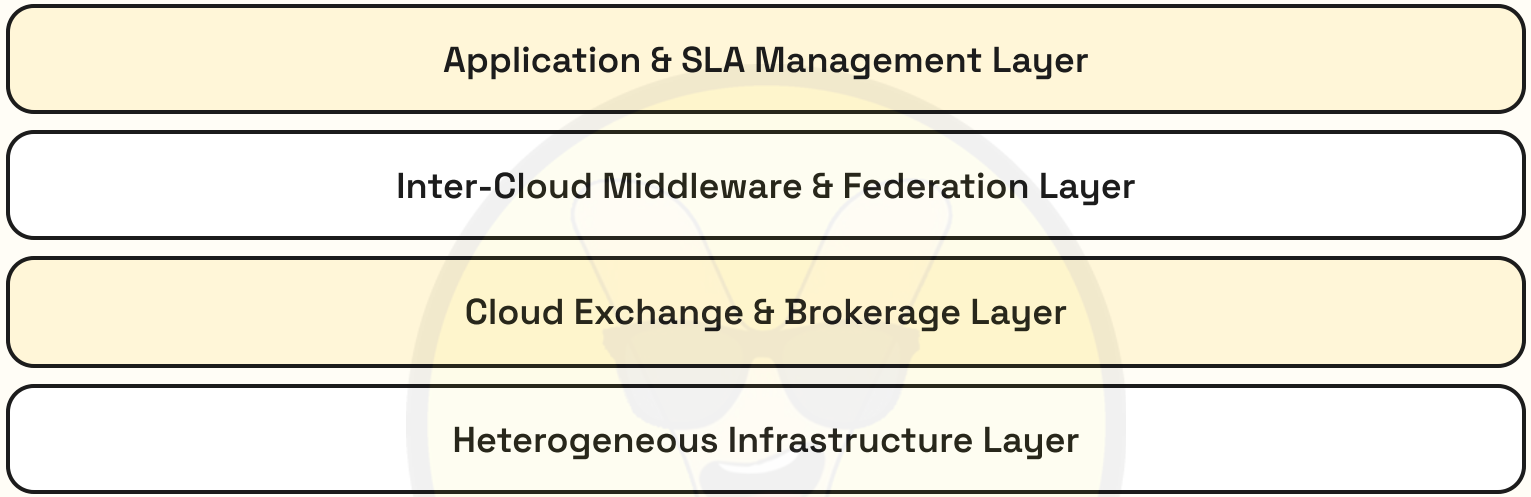
Inter-Cloud Resource Management

INTER-CLOUD RESOURCE MANAGEMENT

A framework that coordinates, provisions, and migrates computing resources across heterogeneous, geographically distributed cloud service providers.

- Prevents vendor lock-in by supporting multi-cloud deployment models.
- Enables cloud bursting during peak workload demands to prevent failure.
- Uses standardized protocols for interoperability and SLA compliance across clouds.

Inter-Cloud Resource Management Architecture

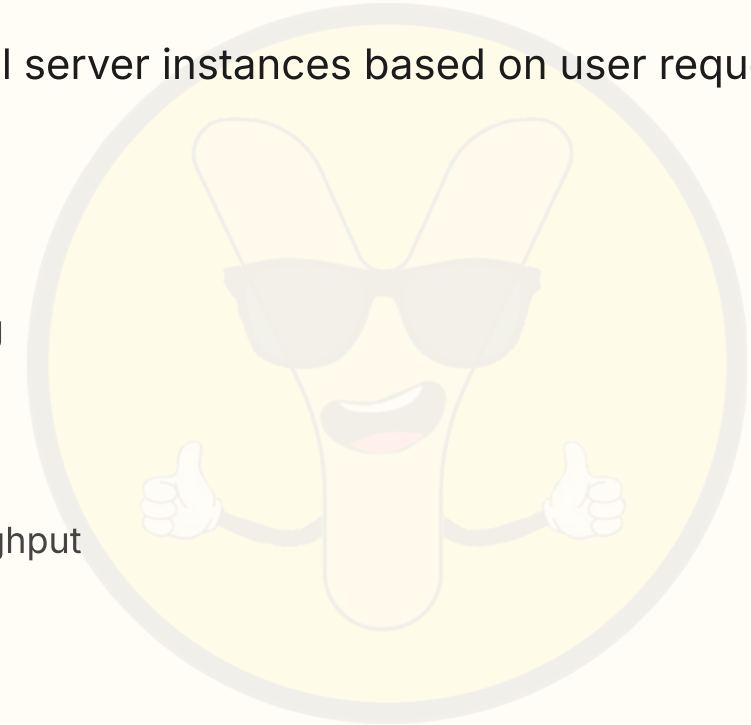


Layered Architecture of Inter-Cloud Resource Management System

Resource Provisioning and Lifecycle

Resource provisioning assigns hardware and software resources to meet performance requirements.

- Mapping cloud services to physical server instances based on user requests.
- Provisioning Phases
  - Resource Discovery & Selection
  - Resource Allocation & Deployment
  - Monitoring & Dynamic Re-provisioning
- Provisioning Metrics
  - Utilization Rate: $U = \frac{R_{used}}{R_{allocated}} \times 100\%$
  - SLA Violation Rate and System Throughput



Comparison of Resource Provisioning Methods

Method	Mechanism	Advantages	Disadvantages
Static Provisioning	Allocates fixed resources based on peak estimated demand	Simple setup, predictable baseline performance	High cost, severe resource under-utilization
Dynamic Provisioning	Allocates/de-allocates resources automatically at runtime	Cost-effective, scales with workload demand	Complex design, potential provisioning latency
User-Driven	User manually selects specific VM configurations	Full control over hardware specification	Requires continuous manual monitoring
Heuristic / Predictive	Uses Machine Learning models to forecast future load	Proactive scaling prevents SLA breaches	Prediction errors lead to over/under provisioning

Worked Example: Dynamic Resource Provisioning

An application needs $R = 100$ computing units. Cloud A charges $\$0.10$ per unit-hour with a 5-minute setup delay. Cloud B charges $\$0.15$ per unit-hour with a 1-minute delay. SLA penalty is $\$5$ per minute of delay. Determine total cost for a 2-hour job.

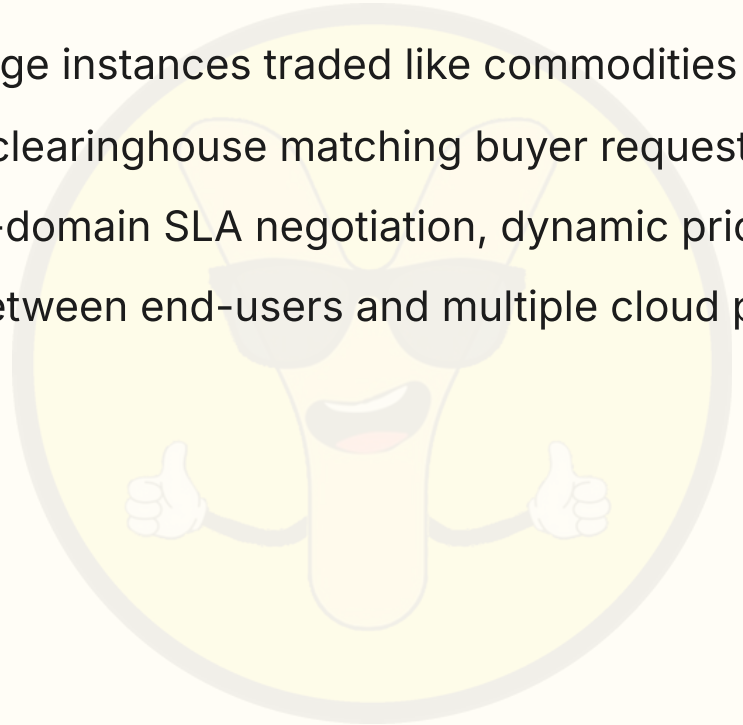
1. Step 1: Compute baseline execution cost for 2 hours (100 units).
2. Cloud A Compute = $100 \times 0.10 \times 2 = \$20.00$
3. Cloud B Compute = $100 \times 0.15 \times 2 = \$30.00$
4. Step 2: Calculate SLA delay penalty cost.
5. Cloud A Penalty = $5 \text{ mins} \times \$5 = \$25.00$
6. Cloud B Penalty = $1 \text{ min} \times \$5 = \$5.00$
7. Step 3: Total Cost = Compute Cost + SLA Penalty
8. Total Cloud A = $\$20.00 + \$25.00 = \$45.00$
9. Total Cloud B = $\$30.00 + \$5.00 = \$35.00$

Cloud B is optimal despite higher hourly rate, yielding a lower total cost of $\$35.00$ due to minimal SLA delay penalty.

Global Exchange of Cloud Resources

A market-driven ecosystem enabling trading of cloud resources between providers.

- Market Trading: Compute and storage instances traded like commodities based on demand.
- Cloud Exchange Market: Acts as a clearinghouse matching buyer requests with provider offers.
- Cloud Coordinator: Manages cross-domain SLA negotiation, dynamic pricing, and resource tracking.
- Cloud Broker: Mediates requests between end-users and multiple cloud providers.



Global Cloud Resource Exchange Workflow



End-to-End Workflow in Global Cloud Resource Trading

Cloud Security Overview

CLOUD SECURITY

A sub-domain of cybersecurity comprising policies, technologies, controls, and services designed to protect cloud data, applications, and infrastructure.

- Confidentiality: Restricting resource access to authorized entities via encryption.
- Integrity: Preventing unauthorized alteration or tampering of data.
- Availability: Guaranteeing continuous accessibility of cloud resources.

Shared Responsibility Security Model

Cloud Service Model	Customer Responsibility	Provider Responsibility
IaaS	OS Patches, Apps, Data, User IAM, Network Rules	Hypervisor, Physical Hardware, Data Center Security
PaaS	Application Code, User Access Controls, Data	Runtime Environment, OS, Middleware, Infrastructure
SaaS	User Data, IAM Roles, Device Security	Entire Stack: Application, OS, Hardware, Network

Cloud Security Challenges

Unique operational properties of clouds introduce complex security threats.

- Multi-Tenancy Vulnerabilities: Data leakage between isolated tenants sharing hardware.
- Insecure APIs: Unprotected management endpoints exposing infrastructure controls.
- Account Hijacking: Compromise of cloud admin credentials resulting in total system control.
- Lack of Visibility: Insufficient monitoring of workloads across multi-cloud environments.
- Data Breaches & Data Loss: Accidental exposure or deletion of sensitive databases.

Software-as-a-Service (SaaS) Security

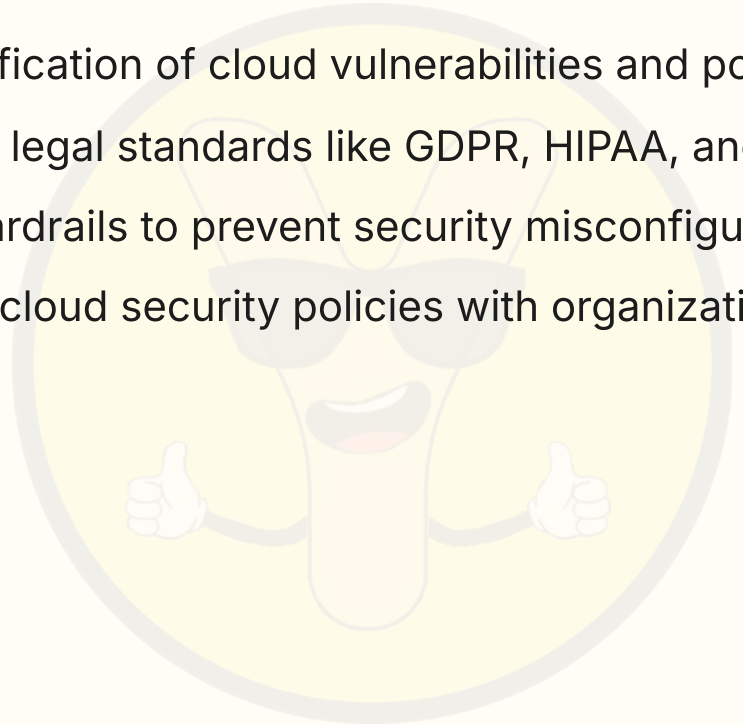
Focuses on securing application software, user interfaces, and data privacy.

- Data Isolation: Multi-tenant database partitioning using logical tenant identifiers.
- Data Encryption: AES-256 for data-at-rest and TLS 1.3 for data-in-transit.
- Identity Governance: Single Sign-On (SSO) combined with Multi-Factor Authentication (MFA).
- CASB Integration: Cloud Access Security Brokers enforce compliance and malware protection.

Cloud Security Governance

Framework establishing administrative rules, risk management policies, and regulatory compliance.

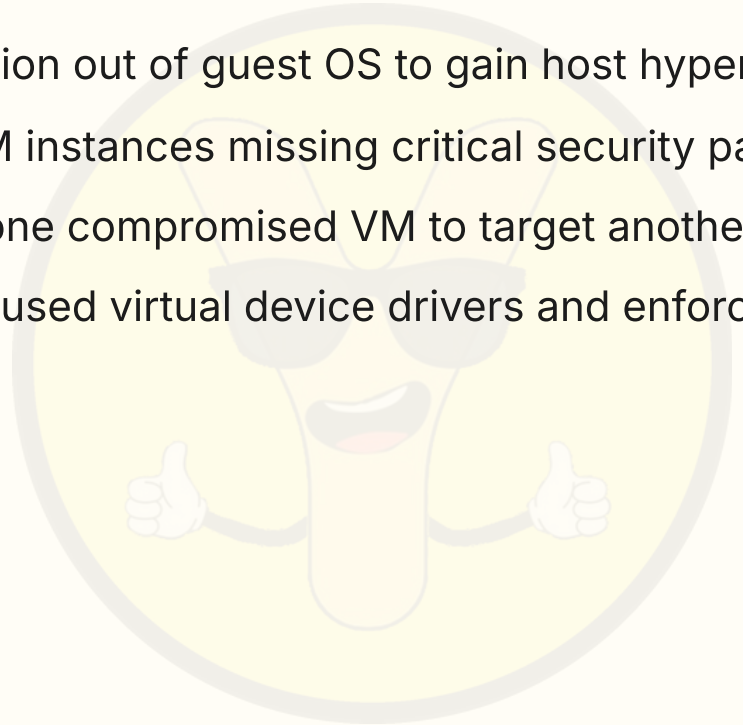
- Risk Assessment: Systematic identification of cloud vulnerabilities and potential business impact.
- Compliance Auditing: Adherence to legal standards like GDPR, HIPAA, and SOC 2.
- Policy Enforcement: Automated guardrails to prevent security misconfigurations.
- Enterprise Alignment: Harmonizing cloud security policies with organizational objectives.



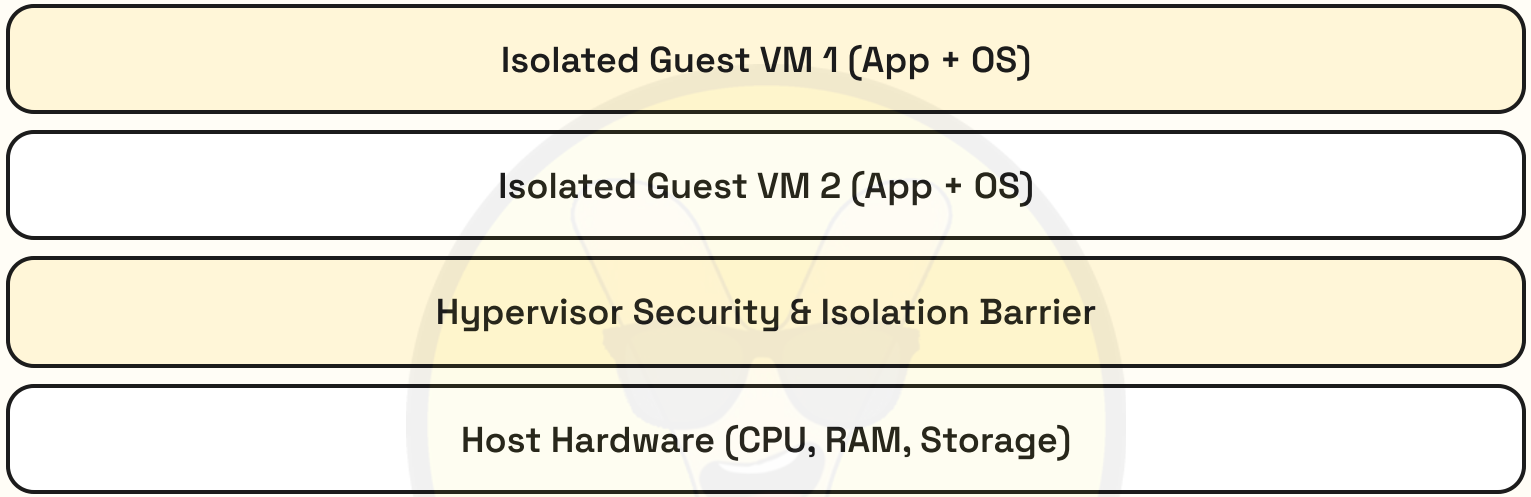
Virtual Machine (VM) Security

Protects virtualized instances and hypervisors from security exploits.

- VM Escape: Attacker breaks execution out of guest OS to gain host hypervisor access.
- VM Sprawl: Unmonitored, active VM instances missing critical security patches.
- VM Hopping: Attacker pivots from one compromised VM to target another VM on the same host.
- Hypervisor Hardening: Disabling unused virtual device drivers and enforcing root integrity.



Hypervisor VM Isolation Architecture



Hypervisor Enforcing Logical Security Boundaries Between VMs

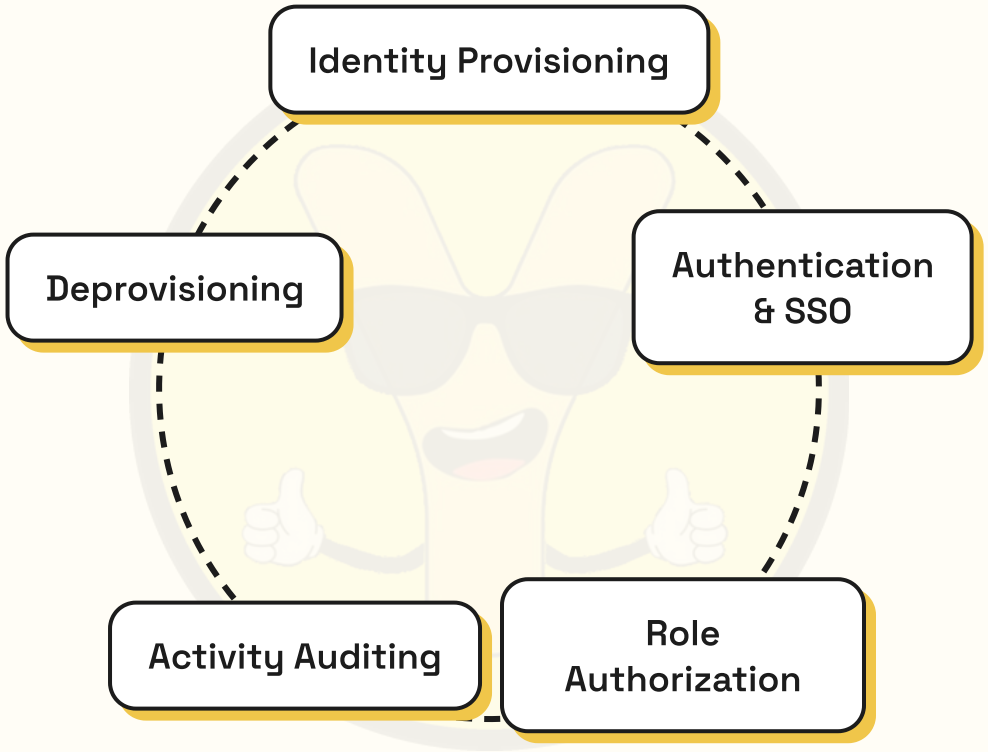
Identity and Access Management (IAM)

IDENTITY AND ACCESS MANAGEMENT (IAM)

A security framework of business processes, policies, and technologies that manages digital identities and controls user access to cloud resources.

- Authentication (AuthN): Verifying user identity via credentials, tokens, or biometrics.
- Authorization (AuthZ): Granting specific permissions using RBAC or ABAC models.
- Accounting: Continuous logging and auditing of user actions for regulatory compliance.

IAM Lifecycle Process



Continuous Lifecycle Management of Cloud Identities

Cloud Security Standards and Frameworks

Standard / Framework	Focus Area	Key Features
ISO/IEC 27017	Cloud Specific Controls	Provides guidelines for cloud security risks and implementation
CSA STAR	Provider Assurance	Three-tiered registry evaluating cloud provider security posture
NIST SP 800-145/53	Security Controls Framework	Defines federal standards for cloud security and privacy controls
PCI-DSS	Payment Data Protection	Mandatory controls for handling credit card information in cloud

Exam Corner: Important Questions

- **Q1** Explain Inter-Cloud Resource Management. Differentiate between static and dynamic resource provisioning methods with examples.
- **Q2** Draw and explain the architecture of Global Exchange of Cloud Resources. What is the role of a Cloud Broker?
- **Q3** Define the Cloud Shared Responsibility Model. Compare security responsibilities across IaaS, PaaS, and SaaS.
- **Q4** What is VM Escape and VM Hopping? Discuss countermeasures for securing hypervisors.
- **Q5** Explain the core components of Identity and Access Management (IAM). Differentiate between RBAC and ABAC.
- **Q6** Write short notes on: (a) ISO/IEC 27017, (b) Cloud Security Governance, (c) SaaS Security Challenges.

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.

