

UNIT 5

Cloud Security

(6 Hours) — Cloud Computing (CACS402)

Disclaimer: These notes were prepared as a study aid and may contain errors or omissions. Please cross-check important definitions, figures and product details (especially vendor services such as Google App Engine, Microsoft Azure and Aneka, which change often) against your prescribed textbook, class notes and official documentation before relying on them in an exam.

5.1 Introduction to Security

Information security is the protection of information and systems from unauthorised access, use, disclosure, disruption, modification or destruction. Its core goals form the **CIA triad**:

Goal	Meaning	Cloud example
Confidentiality	Only authorised parties can read the data.	Encrypting files stored in object storage.
Integrity	Data is accurate and not altered without authorisation.	Checksums and digital signatures on backups.
Availability	Systems and data are accessible when needed.	Multi-zone replication and DDoS protection.

Additional properties: **authentication** (who are you?), **authorisation** (what may you do?), **accountability / non-repudiation** (auditable actions).

Cloud security is the set of policies, technologies and controls that protect cloud data, applications and infrastructure. It operates under a **shared responsibility model**:

	IaaS	PaaS	SaaS
Data & identities	Customer	Customer	Customer
Applications	Customer	Customer	Provider
Runtime / OS	Customer	Provider	Provider
Virtualization / hardware	Provider	Provider	Provider
Physical data centre	Provider	Provider	Provider

Figure 5.1 — Shared responsibility between provider and customer

Note: Exact boundaries vary by provider and service; customers are always responsible for their data, identities and access configuration.

5.2 Cloud Security Challenges and Risks

Risk / challenge	Description
Data breaches and leakage	Sensitive data exposed through misconfiguration (e.g., public storage buckets) or attack.
Insecure interfaces and APIs	Weak authentication or input validation on management/APIs.
Multi-tenancy and isolation failure	Attacker in one VM attempts to reach another tenant (VM escape, side channels).
Loss of control	Customer depends on provider for physical and platform security.
Account hijacking	Stolen credentials give attackers control of cloud resources.
Insider threats	Malicious or careless employees of the customer or provider.
Denial of Service (DoS/DDoS)	Flooding services to make them unavailable or to run up costs.
Vendor lock-in and data portability	Difficulty moving data or applications between providers.
Legal and compliance issues	Data residency, GDPR, audits, e-discovery.
Data remanence	Traces of deleted data remaining on shared storage.

Example 5.1 — Misconfiguration

A company stores customer records in a cloud storage bucket set to “public read”. What type of risk is this and how can it be prevented?

Solution

It is a **data breach through misconfiguration**, a customer-side responsibility.

Prevention: default-deny bucket policies, block-public-access settings, encryption, automated configuration scanning and least-privilege IAM.

5.3 Software-as-a-Service Security

In SaaS the provider runs the application, so customers depend heavily on the vendor’s controls. Customers still control users, data classification and settings.

- **Data security:** encryption at rest/in transit, tenant data segregation, backup and deletion policies.

- **Access control:** SSO, MFA, role-based access, session timeouts.
- **Application security:** secure development (OWASP Top 10), regular patching, penetration testing.
- **Availability and continuity:** SLAs, redundancy, disaster-recovery plans.
- **Compliance and audit:** SOC 2, ISO 27001 reports, audit logs and data-location commitments.
- **Customer tasks:** review vendor security questionnaire, manage user lifecycle, set sharing permissions, use CASB (Cloud Access Security Broker) tools.

5.4 Security Monitoring

Security monitoring continuously collects and analyses logs and events to detect attacks, misuse and policy violations in near real time.

Element	Purpose	Example tools
Logging and audit trails	Record who did what, when, from where.	AWS CloudTrail, Azure Activity Log
SIEM	Correlate logs from many sources and raise alerts.	Splunk, Microsoft Sentinel, ELK
IDS / IPS	Detect/prevent malicious network or host activity.	Snort, Suricata
Vulnerability scanning	Find missing patches and weak configurations.	Nessus, OpenVAS, cloud-native scanners
Configuration and posture management	Detect drift from security baselines.	AWS Config, Defender for Cloud
Incident response	Playbooks to contain, eradicate and recover.	SOC teams, runbooks

- Monitor: failed logins, privilege changes, unusual data downloads, new resources in unexpected regions, sudden cost spikes.
- Keep logs tamper-proof and retain them as required by compliance.

5.5 Security Architecture Design

A secure cloud architecture applies multiple layers of protection so that failure of one control does not expose the system — **defence in depth**.

Layer	Typical controls
Perimeter / network	Firewalls, security groups, WAF, DDoS protection, VPN, private subnets, network segmentation.
Identity	IAM, MFA, SSO, least privilege, privileged-access management.
Host / VM	Hardened images, patching, anti-malware, host firewall.
Application	Secure coding, input validation, API gateways, secrets management.
Data	Classification, encryption, key management (KMS/HSM), backup, DLP.
Governance	Policies, compliance monitoring, audits, risk management.

Design principles

- Least privilege and separation of duties.
- Zero trust — never trust, always verify every request.
- Secure by default and fail-safe defaults.
- Encrypt everything; automate security as code (Infrastructure as Code checks).
- Design for resilience: multi-zone deployment, backups, tested recovery.

5.6 Data Security

Data is the most valuable cloud asset. Data security covers its whole lifecycle: create → store → use → share → archive → destroy.

- **Encryption at rest** (e.g., AES-256) and **in transit** (TLS 1.2/1.3).
- **Key management:** provider-managed keys, customer-managed keys or customer-held keys (BYOK/HYOK); keys stored in KMS/HSM.
- **Data classification and DLP** to detect and block sensitive data leaving the organisation.
- **Backup, replication and versioning** for integrity and availability.
- **Secure deletion:** cryptographic erasure — destroy the key so leftover data is unreadable.
- **Data residency and privacy:** choose regions that satisfy law; anonymise or tokenise personal data.

Example 5.2 — Key management choice

A hospital must ensure that the cloud provider cannot read patient data. What approach is suitable?

Solution

Encrypt data on the client side before upload and keep keys under the hospital's control (customer-managed / hold-your-own-key with an HSM).

The provider stores only ciphertext, reducing confidentiality risk, though some cloud features (indexing, server-side search) become harder.

5.7 Application Security

Cloud applications are exposed to the Internet and must be built and operated securely.

Threat	Prevention
SQL injection	Parameterised queries, input validation, ORM.
Cross-site scripting (XSS)	Output encoding, Content Security Policy.
Broken authentication / session	MFA, secure session tokens, OAuth 2.0 / OpenID Connect.
Insecure APIs	API gateway, authentication, rate limiting, schema validation.
Vulnerable components	Dependency scanning, timely patching, SBOM.
Secrets in code	Use secret managers; never hard-code keys.

- Adopt a **secure SDLC / DevSecOps**: threat modelling, code review, SAST/DAST testing in CI/CD pipelines.
- Use a Web Application Firewall (WAF) and runtime protection; keep containers and images scanned.

5.8 Virtual Machine Security

VMs share physical hardware, so the hypervisor and VM management must be protected.

- **Hypervisor security**: keep it patched, minimal and isolated; restrict management interfaces.
- **VM escape / guest-to-host attacks**: exploit hypervisor bugs to break isolation — mitigated by patching and hardware isolation.
- **Side-channel attacks**: co-resident VMs infer secrets via shared CPU caches; mitigated by isolation and dedicated hosts.
- **VM sprawl and stale images**: forgotten VMs remain unpatched; use lifecycle management.
- **Snapshot and image security**: images may contain secrets or malware; scan and sign them.

- **Network isolation:** virtual firewalls, microsegmentation, separate management network.
- **Inside the VM:** patching, anti-malware, host firewall, disk encryption, monitoring agents.

5.9 Identity Management and Access Control

Identity and Access Management (IAM) ensures the right people and services access the right resources for the right reasons.

Concept	Description
Identification and authentication	Prove identity using passwords, MFA, certificates, biometrics, tokens.
Authorisation	Decide permissions after authentication.
Single Sign-On (SSO)	One login gives access to many services (SAML, OpenID Connect).
Federation	Trust between identity providers and cloud services so external identities can be used.
Provisioning / de-provisioning	Create, update and remove accounts automatically over the user lifecycle.
Auditing	Log and review all access.

Access control models

Model	Basis of decision	Example
DAC — Discretionary	Owner decides who gets access.	File sharing permissions
MAC — Mandatory	System-enforced labels/clearances.	Military classification levels
RBAC — Role-based	Permissions assigned to roles; users get roles.	“Database administrator” role
ABAC — Attribute-based	Policies use user, resource and context attributes.	Allow if department = HR and device is managed

- Apply **least privilege**, enable MFA everywhere (especially for administrators), rotate credentials and review permissions regularly.
- Protocols: OAuth 2.0 (delegated authorisation), SAML and OpenID Connect (authentication/SSO).

Key Takeaways — Unit 5

- ✓ Cloud security protects confidentiality, integrity and availability under a shared responsibility model.
- ✓ Major risks: data breach, misconfiguration, insecure APIs, account hijacking, insider threats, DoS, lock-in and compliance issues.
- ✓ SaaS security relies on vendor controls plus customer-managed users, data and settings.
- ✓ Security monitoring uses logging, SIEM, IDS/IPS and scanning to detect and respond to incidents.
- ✓ Architecture uses defence in depth, least privilege and zero trust; data is protected by encryption and key management.
- ✓ VM security focuses on the hypervisor, isolation and image hygiene; IAM uses authentication, SSO, MFA and RBAC/ABAC.

— *End of Unit 5* —