ABHYASMITRA.IN
STUDY NOTES

CLOUD COMPUTING

Unit IV — Security in Cloud Computing

Topics Covered (09 Hours)

Risks in Cloud Computing & Enterprise-Wide Mitigation
Specific Cloud Risks (Data Breaches, Hacking, Lock-in)
Data Security Challenges in Multi-tenant Infrastructure
Cloud Digital Persona & Identity/Access Management (IAM)
Content Level Security & Encryption Keys Management
Security Services: Confidentiality, Integrity, and Availability
Security Authorization Challenges in Shared Cloud Services
Secure Cloud Software Requirements (SDLC Frameworks)
Secure Software Testing: Static, Dynamic, and Penetration
Security Governance, Audits, & Compliance Standards

Compiled in a simple, easy-to-understand, book style format
for students of Computer Science and Engineering

TABLE OF CONTENTS

4.1 Risks in Cloud Computing & Mitigation 3
Enterprise-Wide Risk Management 3
4.2 Data Security & Digital Persona 4
Encryption & Content Level Security 4
Cloud Digital Persona 4
4.3 Security Services & Software Testing 5
Secure Cloud Software Requirements 5
Secure Cloud Software Testing 5
Unit Summary 6

4.1 Risks in Cloud Computing & Mitigation

Deploying business workloads to the cloud introduces unique security and operational risks. Because organizations surrender physical control of their servers and share resources with other tenants, robust risk management frameworks are essential.

Enterprise-Wide Risk Management

Organizations must perform enterprise-wide risk assessments before migrating data, evaluating regulatory compliance (such as GDPR, HIPAA, or PCI-DSS), financial exposure, and service-level agreements (SLAs). Key risk categories include:

- **Data Breaches & Theft:** Sensitive company or customer data is accessed by unauthorized actors. Since public cloud services are exposed to the internet, weak access credentials can compromise entire datastores.
- **Data Loss:** Data is permanently deleted due to provider error, physical natural disasters at data centers, or malicious encryption by ransomware, requiring robust distributed backup schedules.
- **Vendor Lock-In:** Dependency on a single provider's proprietary APIs, databases, or configurations. If prices rise or service quality drops, migrating applications to another cloud becomes extremely difficult and expensive.
- **Shared Technology Vulnerabilities:** Since virtualization runs multiple VMs on the same hardware, flaws in the hypervisor can allow attackers to perform VM escape, compromising neighboring tenant data.

4.2 Data Security & Digital Persona

Data security in the cloud requires protecting data in three states: Data-at-Rest (stored on disks), Data-in-Transit (moving over networks), and Data-in-Use (processing in memory).

Encryption & Content Level Security

To protect content from unauthorized access, cloud platforms rely heavily on encryption. Content-level security involves encrypting data *before* it leaves the client machine, or using server-side encryption with keys managed in secure hardware modules (like AWS KMS or Azure Key Vault). Strong protocols (such as TLS/SSL) protect data-in-transit, while confidential computing (using hardware-secure enclaves) secures data-in-use.

Cloud Digital Persona

In a cloud environment, a user's digital persona—their digital identity and access privileges—is the primary security perimeter. Traditional network firewalls are insufficient because users access cloud apps from anywhere. Identity and Access Management (IAM) systems manage digital personas by enforcing: Multi-Factor Authentication (MFA), Single Sign-On (SSO), and the Principle of Least Privilege (granting users only the minimum permissions necessary to perform their jobs).

4.3 Security Services & Software Testing

Cloud providers and customers share the responsibility of maintaining the CIA Triad (Confidentiality, Integrity, and Availability) of services.

The CIA Triad in Cloud Computing

Confidentiality: Ensuring that only authorized users have access to data (enforced via encryption and IAM).

Integrity: Ensuring that data is not altered or corrupted during transmission or storage (enforced via hash checksums and digital signatures).

Availability: Ensuring that resources are accessible when needed (enforced via high availability zones, load balancers, and DDoS protection).

Secure Cloud Software Requirements

Software designed for the cloud must integrate security requirements from the start of the software development life cycle (SDLC). Cloud-native applications must support secure session state tokens, dynamic secrets management (never hardcoding passwords in code), and automated compliance auditing.

Secure Cloud Software Testing

Testing cloud-native applications requires validating both the code and the underlying cloud configuration. Essential methodologies include:

- **Static Application Security Testing (SAST):** Analyzing the source code before compilation to detect security flaws (like SQL injections, buffer overflows, or hardcoded secrets).
- **Dynamic Application Security Testing (DAST):** Testing the compiled, running application from the outside, simulating an attacker attempting to exploit active web APIs or endpoints.
- **Penetration Testing:** Simulating real cyberattacks on the entire cloud infrastructure, validating whether security groups, firewalls, and IAM policies successfully block unauthorized entry.

Unit Summary

This unit explored security challenges and risk management in Cloud Computing.

- Cloud risks include data breaches, data loss, vendor lock-in, and shared hypervisor vulnerabilities.
- Data security relies on encrypting data at-rest, in-transit, and in-use, combined with KMS key management.
- A user's digital persona is secured using IAM systems, MFA, and least privilege policies.
- Security services guarantee Confidentiality, Integrity, and Availability (the CIA Triad).
- Secure cloud software development integrates security requirements throughout the SDLC.
- Testing methodologies include SAST (code analysis), DAST (runtime tests), and penetration testing.