CC ENDSEM UNIT – 5 PYQ

➢ MAY / JUN 2022

Q5

a) Explain the different Cloud Security Services in detail [9]

Cloud Security Services

Cloud Security Services are essential to ensure confidentiality, integrity, and availability of data and applications hosted on cloud platforms. These services help protect cloud infrastructure, data, and operations from cyber threats.

1. Identity and Access Management (IAM)

- Controls who can access what in the cloud.
- Ensures only authorized users can access cloud resources. Includes features like multi-factor authentication (MFA), role-based access control (RBAC), and single sign-on (SSO).
- Example: AWS IAM, Azure Active Directory.

2. Data Encryption

- Protects data at rest, in transit, and in use.
- Uses cryptographic techniques to prevent unauthorized access.
- Symmetric and asymmetric encryption, key management, and TLS/SSL protocols are used.
- Example: AWS Key Management Service (KMS), Google Cloud Key Management.

3. Firewall and Network Security

- Protects cloud infrastructure from unauthorized network access.
- Includes virtual firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs.
- Helps control inbound/outbound traffic and protect against DDoS attacks.
- Example: AWS WAF, Azure Firewall.

4. Security Information and Event Management (SIEM)

- Collects and analyzes logs from various sources to detect threats and anomalies.
- Provides real-time monitoring, alerting, and incident response.
- Helps in auditing and compliance.
- Example: Splunk, IBM QRadar, Azure Sentinel.

5. Data Loss Prevention (DLP)

- Prevents sensitive data from being **l**eaked or accessed inappropriately.
- Monitors and controls data transfer to ensure **data security policies** are followed.
- Example: Microsoft 365 DLP, Symantec DLP.

6. Endpoint Security

- Secures user devices (laptops, smartphones) that access cloud services.
- Includes antivirus, anti-malware, and device management policies.
- Helps prevent threats that originate from compromised endpoints.
- Example: CrowdStrike, Microsoft Defender for Endpoint.

7. Compliance and Risk Management

- Ensures cloud usage complies with regulatory standards (e.g., GDPR, HIPAA).
- Helps in assessing, managing, and mitigating security risks.
- Tools offer compliance reports and automatic checks.
- Example: AWS Artifact, Azure Compliance Manager.

b) What are different risks in cloud computing and how to mange them? [9]

1. Data Breaches

- **Risk**: Unauthorized access to sensitive data due to weak access control or attacks.
- **Management**:
    - Use strong encryption (data at rest and in transit).
    - Implement multi-factor authentication (MFA) and role-based access.
    - Conduct regular security audits and monitoring.

2. Data Loss

- **Risk**: Permanent loss of data due to accidental deletion, corruption, or hardware failure.
- **Management**:
    - Set up automated backups and disaster recovery plans.

- Use redundant storage and geo-replication.
- Validate backup restoration periodically.

3. Insecure APIs

- **Risk**: Vulnerabilities in APIs may allow attackers to gain control over cloud services.
- **Management**:
  - Use secure coding practices.
  - Implement API gateways, authentication, and rate limiting.
  - Regularly test and patch vulnerabilities.

4. Insider Threats

- **Risk**: Malicious or careless insiders can leak or misuse data.
- **Management**:
  - Enforce least privilege principle.
  - Monitor user activities and maintain audit logs.
  - Conduct security awareness training.

5. Account Hijacking

- **Risk**: Attacker gains control over cloud accounts via phishing or weak credentials.
- **Management**:
  - Use strong passwords, MFA, and session timeouts.
  - Monitor for unusual login behavior.
  - Educate users against phishing attacks.

6. Lack of Compliance

- **Risk**: Failure to meet regulatory standards like GDPR, HIPAA.
- **Management**:
  - Choose cloud providers with compliance certifications.
  - Use compliance tools and templates.

- Maintain documentation and logs for audits.

7. Denial of Service (DoS) Attacks

- **Risk**: Overloading cloud resources to disrupt services.

- **Management**:
  - Use DDoS protection services.
  - Set up auto-scaling and traffic filtering.
  - Monitor network traffic for anomalies.

Cloud risks can be effectively managed through strong security policies, regular monitoring, secure architecture, and user education, ensuring safe and reliable cloud operations.

Q6)

a) Explain security authorization challenges in cloud computing? [9]

1. **Multi-Tenancy:**
   - Multiple users share the same infrastructure, making it challenging to enforce strict and isolated access control policies.
2. **Dynamic Scaling and Elasticity:**
   - Resources are dynamically allocated and deallocated, requiring real-time authorization updates, which complicates enforcement.
3. **Identity Management:**
   - Users may have different identities across multiple cloud services, making unified and secure authorization difficult.
4. **Access Control Models:**
   - Implementing proper Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), or Policy-Based Access Control (PBAC) across various cloud layers can be complex.
5. **Delegation of Access:**
   - Cloud users often need to delegate access to third parties, raising concerns about fine-grained access rights and revocation mechanisms.

6. **Cross-Domain Authorization:**
    - Hybrid and multi-cloud setups require federated identity and authorization across platforms, which is error-prone and security-critical.
7. **Data Location and Jurisdiction:**
    - Legal constraints based on data locality may affect who can access which data and how authorization is granted.

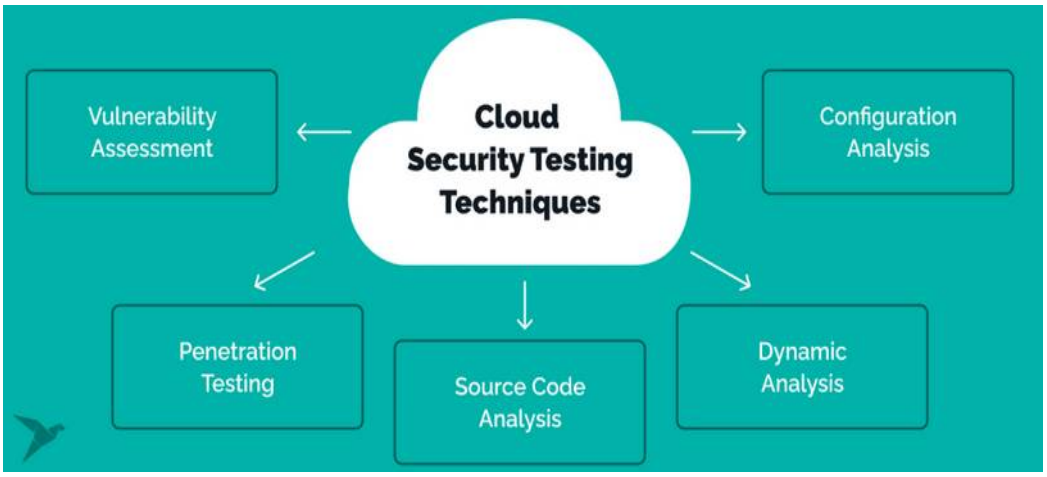
8. **Insider Threats:**
    - Malicious insiders with privileged access may bypass authorization controls and misuse data or resources.
9. **Audit and Compliance:**
    - Ensuring traceable and compliant access control for auditing purposes across different cloud providers is challenging.

Cloud authorization challenges arise from dynamic environments, multi-user access, and lack of transparency. Effective solutions include implementing strong access controls, using identity federation, monitoring systems, and adhering to compliance standards.

“Cloud platforms like Salesforce use federated authentication via SAML and delegated LDAP models to manage access securely.”

b) Discuss how we need to perform secure cloud software testing? [9]

Secure cloud software testing ensures that cloud-based applications and platforms are resilient against security threats such as data breaches, unauthorized access, and misconfigurations. The goal is to detect vulnerabilities early and ensure compliance with security standards.



1. Threat Modeling

- Identify potential threats and attack surfaces in the cloud environment.
- Focus on entry points like APIs, storage, and user access.

2. Security Requirements Testing

- Verify whether the system meets confidentiality, integrity, and availability (CIA) goals.
- Ensure compliance with regulations like GDPR or HIPAA.

3. Vulnerability Scanning

- Use automated tools to detect known security flaws.
- Scan cloud VMs, containers, APIs, and applications regularly.

4. Penetration Testing

- Simulate real-world attacks to uncover weaknesses.
- Focus on testing authentication, access control, and data handling.

5. Identity and Access Management (IAM) Testing

- Test role-based access control, multi-factor authentication, and session handling.
- Ensure only authorized users can access resources.

6. Data Security Testing

- Verify encryption of data at rest and in transit.
- Check for proper key management and secure data access controls.

7. Configuration Testing

- Ensure cloud configurations are secure (e.g., no open storage buckets, default credentials).
- Identify and fix misconfigurations in services or resources.

8. Logging and Monitoring Validation

- Test whether security events are properly logged.
- Ensure alerts are generated for suspicious or unauthorized activities.

9. Security Regression Testing

- Re-test fixed vulnerabilities to confirm they have not reappeared.
- Run tests after updates or patches to ensure new issues haven't been introduced.

Secure cloud software testing is a continuous and systematic process. It combines vulnerability detection, access control validation, and compliance checks to ensure cloud applications remain secure and trustworthy.

➢ **NOV / DEC 2022**

Q5

a) What are the security issues of cloud computing identified by Cloud Security Alliance (CSA)? Explain any three in detail [9]

Security Issues Identified by Cloud Security Alliance (CSA)

The **Cloud Security Alliance (CSA)** has identified a list of **Top Threats to Cloud Computing**, commonly referred to as the "**Notorious Nine**." These are the most critical security concerns in cloud environments.

List of Security Issues by CSA:

1. Data Breaches
2. Data Loss
3. Account or Service Hijacking
4. Insecure APIs
5. Denial of Service (DoS)
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Vulnerabilities

Explain Any Three in Detail:

1. Data Breaches

- **Description**: Unauthorized access to sensitive data stored in the cloud.
- **Causes**: Weak authentication, misconfigured access controls, or insecure APIs.
- **Impact**: Loss of customer trust, legal penalties, and reputational damage.
- **Example**: A public S3 bucket exposing confidential client data.

2. Account or Service Hijacking

- **Description**: Attackers steal credentials to gain unauthorized access to cloud accounts.
- **Causes**: Phishing, weak passwords, or stolen tokens.
- **Impact**: Attacker may eavesdrop, manipulate data, or redirect clients to malicious sites.
- **Mitigation**: Multi-Factor Authentication (MFA), strong password policies, monitoring login activity.

3. Insecure APIs

- **Description**: APIs are used to manage cloud services, but if not properly secured, they can be exploited.

- **Causes**: Poorly coded or publicly exposed APIs without proper authentication.
- **Impact**: Unauthorized access, data leaks, and full service compromise.
- **Mitigation**: Secure coding practices, rate limiting, API gateways, and proper access controls.

The CSA's identified threats highlight the importance of implementing strong security measures in cloud environments. Addressing these issues is critical for maintaining trust, compliance, and system integrity

b) How Trusted Cloud Computing can be used to manage the risk and security in a cloud? [9]

Trusted Cloud Computing refers to designing cloud systems that ensure security, reliability, and user confidence by using trusted technologies, policies, and frameworks.

It focuses on **protecting data, identities, and infrastructure** from threats while ensuring compliance and transparency.

How TCC Helps Manage Risk and Security in Cloud:

1. Hardware-Based Trust (Trusted Platform Module - TPM)

- TPMs ensure that the system boot process and hardware configuration are **secure and untampered**.
- Verifies **hardware integrity** before software runs, reducing risks from rootkits and malware.

2. Secure Virtualization

- Ensures isolation between tenants using hypervisors with trusted computing features.
- Prevents VM-level attacks and data leakage in multi-tenant environments.

3. Attestation Mechanisms

- Allows users to **verify the cloud provider's infrastructure** (e.g., software stack, configurations).
- Builds **transparency and trust** through remote attestation.

4. Encrypted Storage and Communication

- TCC enforces **end-to-end encryption** for data at rest and in transit.

- Ensures **confidentiality** even if cloud servers are compromised.

5. Identity and Access Control

- Uses **strong authentication**, role-based access, and identity federation.
- Reduces risk of **unauthorized access** and **account hijacking**.

6. Policy Enforcement and Auditing

- Enables **automatic enforcement of security policies** and **audit trails** for accountability.
- Helps in **compliance with standards** like GDPR, HIPAA.

7. Trusted Software Execution

- Ensures applications and services run in a **verified and secure environment**.
- Prevents the use of **malicious or unauthorized software**.

Trusted Cloud Computing enhances cloud security by combining **secure hardware, software, and policies** to ensure **data protection, integrity, and transparency**. It builds trust between cloud providers and users while effectively managing risks.

Q6

a) Explain the six-step risk management process [9]

Risk management is a structured approach used to identify, evaluate, and mitigate risks that could negatively impact an organization. The six-step process ensures that potential threats are managed systematically.

1. Determine the Objectives

- Define what the risk management process aims to achieve.
- Objectives often include ensuring business continuity, minimizing losses, and protecting assets.

2. Identify the Risks

- Recognize internal and external risks that may affect the organization.
- Tools used: risk analysis questionnaires, interviews, inspections, and checklists.

3. Evaluate the Risks

- Assess the likelihood and impact of each identified risk.
- Prioritize risks as critical, significant, or low-level based on severity and probability.

4. Consider Alternatives and Select Risk Treatment

- Choose risk management strategies: avoidance, reduction, sharing, or acceptance.
- Select the most appropriate method based on cost, impact, and feasibility.

5. Implement the Decision

- Apply the chosen risk treatment measures.
- Allocate resources and assign responsibilities for effective execution.

6. Evaluate and Review

- Continuously monitor the risk environment and effectiveness of controls.
- Revise the strategy as needed to adapt to new or evolving risks.

The six-step risk management process helps organizations handle uncertainties proactively by providing a clear framework to identify, assess, and address risks effectively.

b) Describe how to perform Secure Cloud Software Testing? [9]

→ **already done !!**

➢ **MAY / JUN 2023**

Q5)

a) What are the different types of testing in cloud computing? Explain briefly? [9]

Types of Testing in Cloud Computing

1. **Functional Testing:**
   Tests whether cloud applications perform their intended functions correctly according to requirements, including workflows and user interactions.
2. **Performance Testing:**
   Measures the speed, responsiveness, scalability, and stability of cloud services under various workloads, including load and stress testing.
3. **Security Testing:**
   Ensures cloud applications and infrastructure are protected from threats like unauthorized access, vulnerabilities, and data breaches by penetration testing and vulnerability scanning.
4. **Compatibility Testing:**
   Verifies that cloud applications work correctly across different devices, browsers, operating systems, and network environments.
5. **Disaster Recovery Testing:**
   Tests the ability of cloud systems to recover data and resume normal operations after a failure or disaster.
6. **Data Integrity Testing:**
   Confirms that data stored and processed in the cloud remains accurate, consistent, and uncorrupted.
7. **Compliance Testing:**
   Checks that cloud services meet legal and regulatory standards such as GDPR, HIPAA, and PCI-DSS.
8. **Migration Testing:**
   Ensures that applications and data successfully move from on-premises or other cloud platforms to the new cloud environment without loss or corruption.
9. **Usability Testing:**
   Evaluates the user interface and overall user experience of cloud applications for ease of use and accessibility.

b) Explain the different types of security risk involved in cloud computing? [9]

Types of Security Risks in Cloud Computing

Cloud computing introduces various security risks due to its shared, distributed, and remote-access nature. These risks affect data, applications, and infrastructure hosted in the cloud.

1. Data Breaches

- Unauthorized access to sensitive data stored in the cloud.
- May occur due to weak access controls, poor encryption, or misconfigured storage.

2. Data Loss

- Permanent loss of data due to accidental deletion, hardware failure, or lack of backup.
- Can result from human error or malicious attacks like ransomware.

3. Account or Service Hijacking

- Attackers gain control over user accounts through phishing, weak credentials, or session hijacking.
- Leads to unauthorized operations and data manipulation.

4. Insecure APIs

- Application Programming Interfaces used to access cloud services may be poorly secured.
- Vulnerabilities can allow attackers to manipulate or steal data.

5. Insider Threats

- Malicious or careless internal users misusing their access to harm the system.
- Hard to detect and can lead to major data leaks or system damage.

6. Denial of Service (DoS) Attacks

- Attackers flood cloud services with traffic to make them unavailable.
- Disrupts service availability and affects legitimate users.

7. Shared Technology Vulnerabilities

- Multi-tenancy and resource sharing in cloud environments may expose clients to each other.

- Weak isolation mechanisms can lead to unauthorized access.

8. Compliance and Legal Risks

- Failure to meet data protection laws (e.g., GDPR, HIPAA) may result in penalties.
- Cloud providers and users share responsibility for compliance.

9. Misconfiguration Risks

- Incorrectly set permissions, open databases, or default credentials can expose systems.
- Common due to complex cloud settings and lack of user expertise.

Understanding and managing these security risks is critical for safe and effective use of cloud computing. Organizations should adopt strong security policies, monitoring, and user education to reduce these threats.

Q6)

a) Describe the different Cloud Security Services in detail? [9]

→ Already done !!

b) State the use of Content Level Security (CLS)?

Content Level Security (CLS) refers to the protection of data based on its **sensitivity and context**, ensuring that only authorized users can access or manipulate specific content within an application or system.

Uses of Content Level Security (CLS):

1. Granular Access Control

- CLS allows access control at a fine-grained level, such as individual documents, records, or fields.
- Users can view or edit only the content that is relevant to their roles.

2. Improved Data Protection

- Sensitive content (e.g., financial data, personal information) is secured using encryption and access rules.
- Reduces the risk of data leakage or unauthorized exposure.

3. Multi-Tenant Isolation

- In cloud applications serving multiple organizations, CLS ensures **data segregation**.
- Each tenant sees and accesses only their own content.

4. Role-Based Data Access

- Users are assigned roles (e.g., admin, manager, staff), and each role has **specific permissions** over content.
- Prevents unauthorized actions like deletion or modification.

5. Dynamic Content Filtering

- CLS dynamically filters and presents only the **permitted data** to the user based on their access level.
- Enhances both **security** and **user experience**.

6. Regulatory Compliance

- CLS helps organizations comply with **data protection regulations** (like GDPR, HIPAA) by controlling who can access what.
- Ensures **audit trails and policy enforcement**.

7. Simplified Application Management

- Applications need not run on multiple servers or have duplicated modules for different roles.
- A single platform can manage **diverse content securely** using CLS.

Content Level Security is crucial for securing cloud-based applications by enforcing data access policies at a detailed level, thereby minimizing risk and enhancing compliance and operational efficiency.

➢ **NOV / DEC 2023**

Q5)

a) Explain the different Cloud Security Services in detail? [9]

b) State the use of Content Level Security (CLS)? [9]

Q6)

a) What are the different types of testing in cloud computing? Explain briefly? [9]

b) Analyze the different types of security risk involved in cloud computing? [9]

!! ALL ARE ALREADY COVERED !!

➢ **MAY / JUN 2024**

Q5)

a) What is role of Confidentiality, Integrity and Availability in Cloud Computing? [6]

Role of Confidentiality, Integrity, and Availability (CIA) in Cloud Computing

The **CIA triad** is the foundation of cloud security. It ensures that cloud services are **secure, reliable, and trustworthy** for users and organizations.

1. Confidentiality

- Ensures that only authorized users can access sensitive data.
- Achieved through encryption, access control, and authentication mechanisms.
- Prevents data leaks and unauthorized exposure.

2. Integrity

- Ensures that data is accurate, consistent, and unaltered during storage or transmission.
- Protected using hash functions, checksums, and version control.
- Prevents tampering or accidental corruption.

3. Availability

- Ensures that **data and services are accessible** to authorized users whenever needed.
- Achieved through **redundancy, load balancing**, and **disaster recovery plans**.
- Prevents downtime and service disruption.

Conclusion:

The CIA triad plays a critical role in maintaining **trust, functionality, and compliance** in cloud computing. All three elements must be balanced to provide secure and effective cloud services.

b) Explain types of Risks in Cloud Computing? [6]

→ already done !

c) Explain the secure cloud software testing? [6]

→ already done !

Q6)

a) Explain the cloud security services in details? [6]

→ already done !

b) Write a short note on content level security? [6]

→ already done !

c) Compare server side and client-side encryption? [6]

Aspect	Server-Side Encryption (SSE)	Client-Side Encryption (CSE)
Where encryption occurs	Performed by the **cloud service provider**	Performed by the **client before uploading data**
Key management	Managed by the **cloud provider**	Managed by the **client/user**
Control over data	Less control; provider handles encryption and decryption	More control; only client holds the decryption keys
Ease of use	Easier to implement; integrated with cloud services	More complex; requires user-side tools and key handling
Security level	Depends on provider's security policies	Considered more secure, as providers cannot access data
Use case	Suitable for general cloud storage	Preferred for **highly sensitive or regulated data**

- **NOV / DEC 2024**

Q5)

a) What are the security issues of cloud computing identified by Cloud Security Alliance (CSA)? Explain any three in detail? [9]

b) How Trusted Cloud Computing can be used to manage the risk and security in a cloud? [9]

Q6)

a) Describe the six step risk management processes? [9]

b) Describe how to perform Secure Cloud Software Testing? [9]

!! ALL QUESTIONS ARE ALREADY COVERED !!