MULTI ATOMS

Page No.:
Date : / /

Cloud Computing

Unit - 4

KCS - 713

Topics →
- Intra - Cloud Resource Management.
- Resource Provisioning & Methods.
- Global Exchange of Cloud Resources
- Security Overview
- Cloud Security Challenges
- Software - as - a Service Security
- Security Governance
- Secure SDLC
- Virtual Machine Security.
- IAM Cloud
- Security standards.
- Honeypots & its types.

[AKTU - 2023-24]

What is Inter-Cloud Resource Management ?

→ Inter-cloud resource management is about using resources (like storage or computing power) from many different cloud providers instead of just one.

→ This helps when one cloud doesn't have enough resources or runs into limits, allowing it to "borrow" resources from other clouds.

→ You can think of it like a group of clouds working together, helping each other out when one cloud can't handle the demand.

Need of Inter-Cloud Resource Management

1. **Running Out of Resources** :- A cloud might use up all its storage or computing power, making it unable to serve more customers.

2. **Avoiding Downtime** :- If one cloud has a problem (like down time), businesses can switch to another cloud for uninterrupted service.

3. **Vendor Lock-In** :- Businesses don't want to depend on just one cloud provider for everything. Inter-cloud resource management lets them use different clouds & avoid being stuck with just one provider.

Page No.:
Date : / /

Benefits of Inter-Cloud Resource Management

1. More flexibility
2. Global Reach.
2. Better Service
3. On-Demand Growth.

Types of Inter-Cloud Resource Management

1. Federation clouds :

→ Multiple cloud providers connect their systems and share resources with each other.
→ Governments or private companies might use this to combine their clouds for better cooperation.

2. Multi-Cloud :

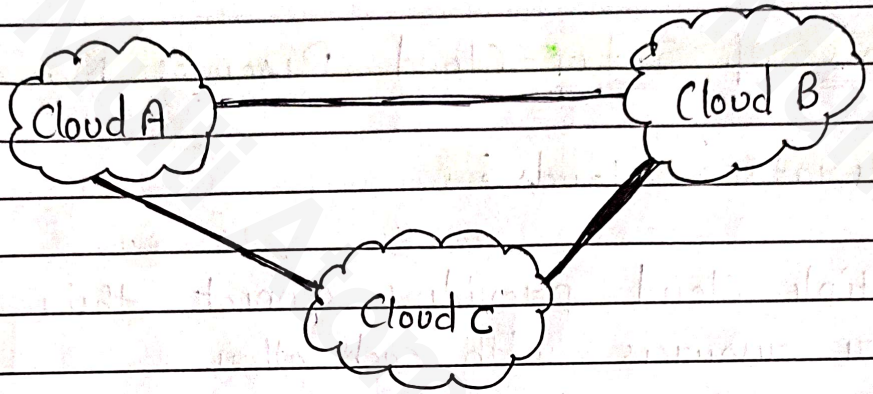
→ A business or client uses multiple clouds but manages them separately. These clouds don't share resources with each other; instead, the client manages which cloud to use for what.
→ A company might use Amazon Web Services (AWS) for storage & Microsoft Azure for computing power.

Date: / /

How Inter-Cloud Architecture work

1. Peer-to-Peer Cloud Federation

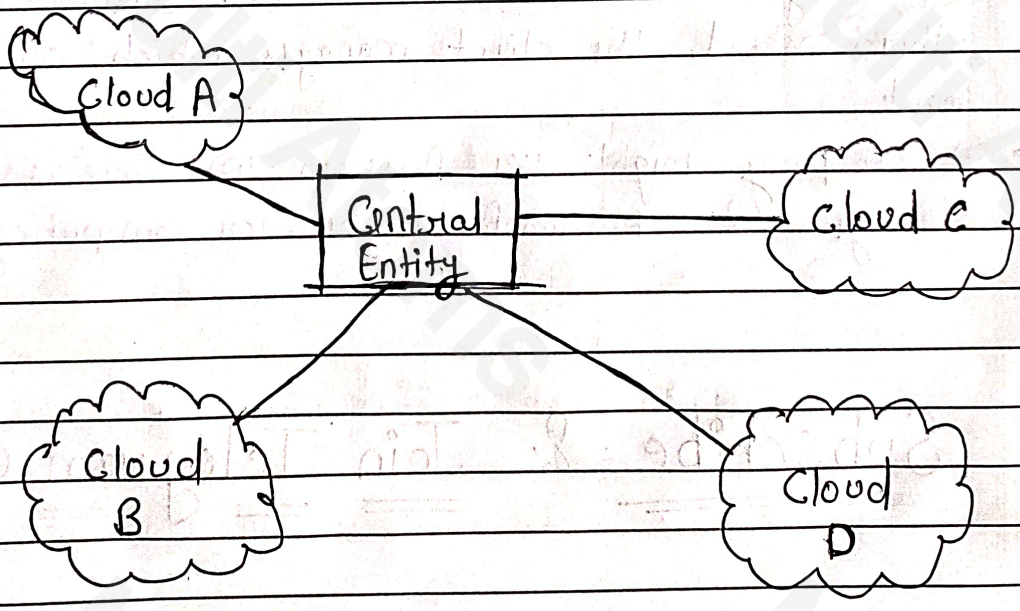
→ Clouds talk to each other directly, without any middleman, to share resources.



2. Centralized Cloud Federation:

→ A central system controls & manages how clouds share resources.

→ ex→ Dynamic Cloud Collaboration

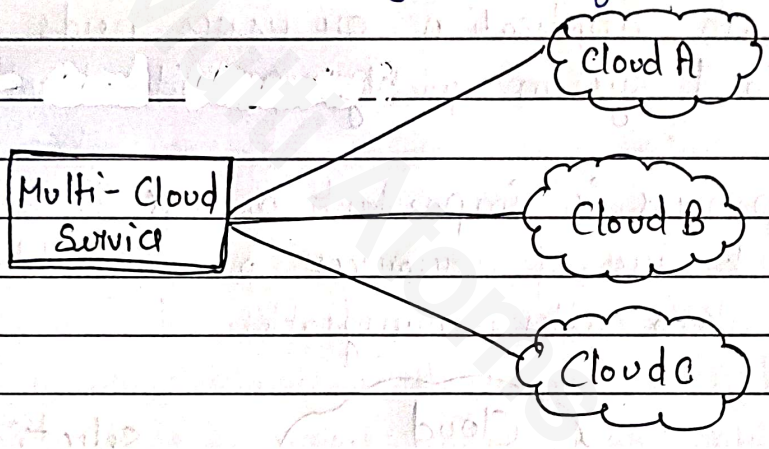


Page No.:
Date: / /

3. Multi-Cloud Services :

→ A service (like a broker) helps a client access multiple clouds.

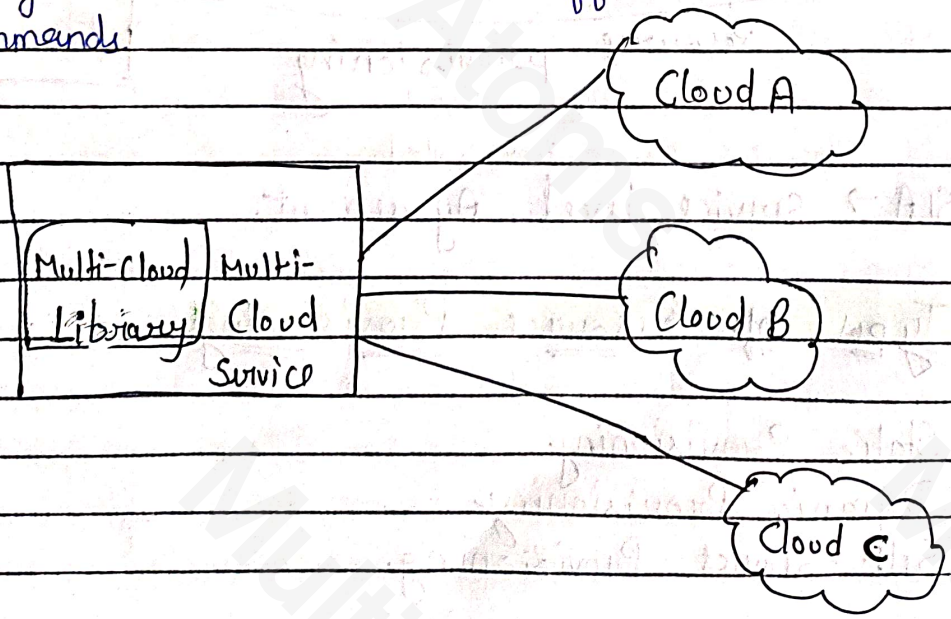
→ Services like OPTIMUS and STRATOS make it easier to use multiple clouds through one system.



4. Multi-Cloud Libraries :

→ Developers use libraries (sets of code) to manage multiple clouds in a consistent way.

→ Libraries like JClouds and Apache libcloud let programmers work with different clouds using the same commands.

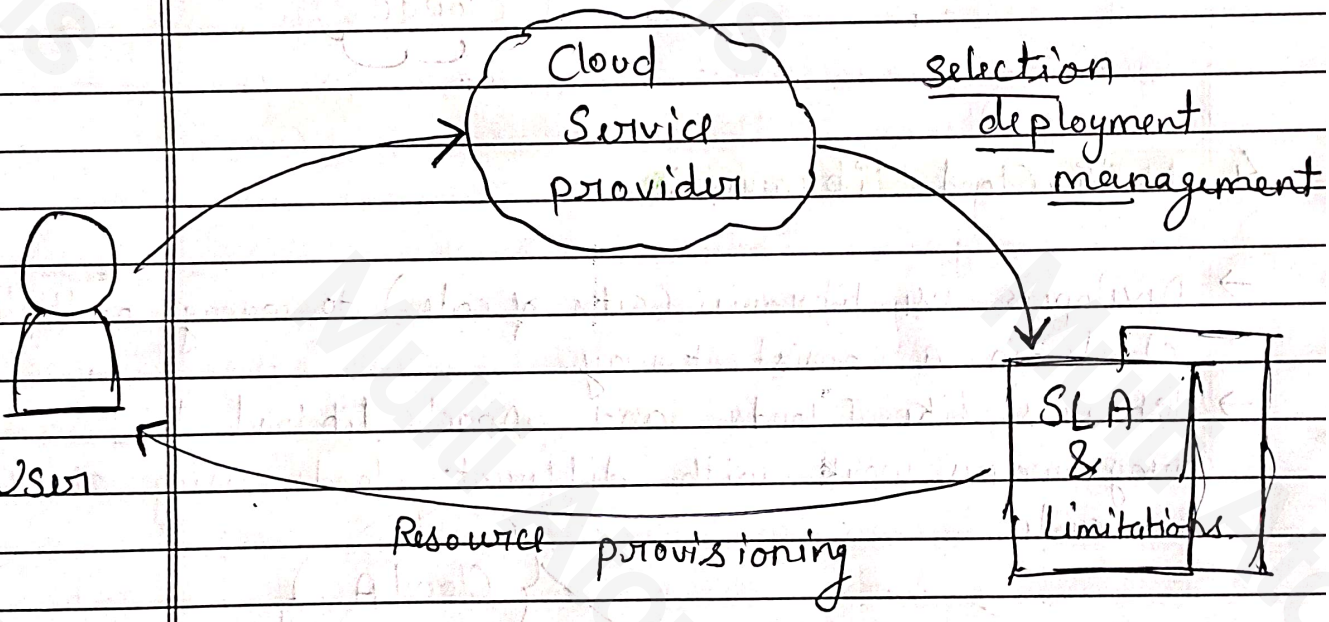


AKTU - [2022-23] [2023-24]

Resource Provisioning ?

Resource provisioning is the act of preparing and allocating resources (choosing, deploying & manage) in a cloud environment. When an application or user needs resources, the cloud system quickly provides them.

This process is important because it ensures efficient use of resources, prevents delays & helps keep costs manageable.



SLA → Service level Agreement.

* Types of Resource Provisioning

i. Static Provisioning
ii. Dynamic Provisioning
iii. Self-Servicd Provisioning.

Page No.:
Date: / /

1. Static Provisioning (or Advance Provisioning):

→ Resources are allocated in a fixed amount, based on the customer's known needs.
→ Works well for applications with steady resource needs.
→ Challenges ⇒ Can lead to over-provisioning or under-provisioning.

2. Dynamic Provisioning (or On-Demand Provisioning):

→ Resources are allocated based on real-time needs. If demand increases, more resources are added, and if demand decreases, resources are scaled down. This method follows a pay-as-you-go model.

→ Ideal for applications with unpredictable demand, allowing users to pay only for what they use.

→ Challenges ⇒ Requires constant monitoring to avoid oversubscription, which can increasing costs.

3. Self-Service Provisioning (or User Self-Provisioning):

→ Users can directly request resources from the cloud provider through a Self-Service portal. They can set-up an account and pay and resources are provided almost instantly.
→ Challenges : Users must manage their own resources to avoid overspending.

AKTU - 2022-23

Q. Illustrate the following in detail

i) Demand - Driven Resource Provisioning.
ii) Event - Driven Resource Provisioning.

Ans Demand - Driven Resource Provisioning

It adjusts resources based on actual demand. when more resources are needed, they are automatically added; when less is needed, resources are scaled down.

e.g for e-commerce websites or streaming services.

Key features. → Usage Monitoring
→ Automic Scaling
→ Cost Efficiency.

Event - Driven Resource Provisioning

It allocates in response to specific events, rather than constant demand monitoring. These events can be scheduled or sudden.

Key features → Quick Response to Events
→ Predefined Rules.
→ Improved System Efficiency.
→ Trigger-Based (eg sign-up)

Page No.:
Date: / /

Types

1) Scheduled Events → for specific Event
2) Unscheduled Events. → Unexpected like social media post going viral

* Global Exchange of Cloud Resources.

→ It is the system designed to bring together different cloud providers, enabling them to share resources dynamically across multiple geographical regions.

→ It allows cloud providers, users & intermediaries (like brokers) to interact and trade resources dynamically based on supply, demand and market conditions.

→ It helps maintain reliability, even during site-specific failures.

→ Think of the Global Exchange of Cloud Resources like a big marketplace for cloud services.

1. Cloud providers (like AWS, Google Cloud, Microsoft Azure): have storage, computing power, and other resources to offer.

2. Customers (companies or individuals): need these resources to run their applications, store, data or perform heavy processing tasks.

Page No.
Date: / /

Just as a farmer's market has different vendors with vegetables, fruits & grains this cloud marketplace has different providers with computing resources to share.

Why Do We Need a Global Cloud Exchange?

→ Each cloud provider has its own data centers around the world. But, even a large provider like AWS can't build data centers in every country or handle unlimited demand on its own.

→ Sometimes, customers might need extra resources in a specific area or when their demand unexpectedly goes up.

→ To solve this problem, cloud providers join together in a global exchange where they can share and trade resources with each other.

1. Cloud Exchange (CEx)

→ This is like the central marketplace or platform where cloud providers can buy & sell resources.

→ Providers publish what resources they have available, & the exchange matches these with customer needs.

→ The CEx makes sure there are competitive prices & helps to manage resource demand & supply efficiently.

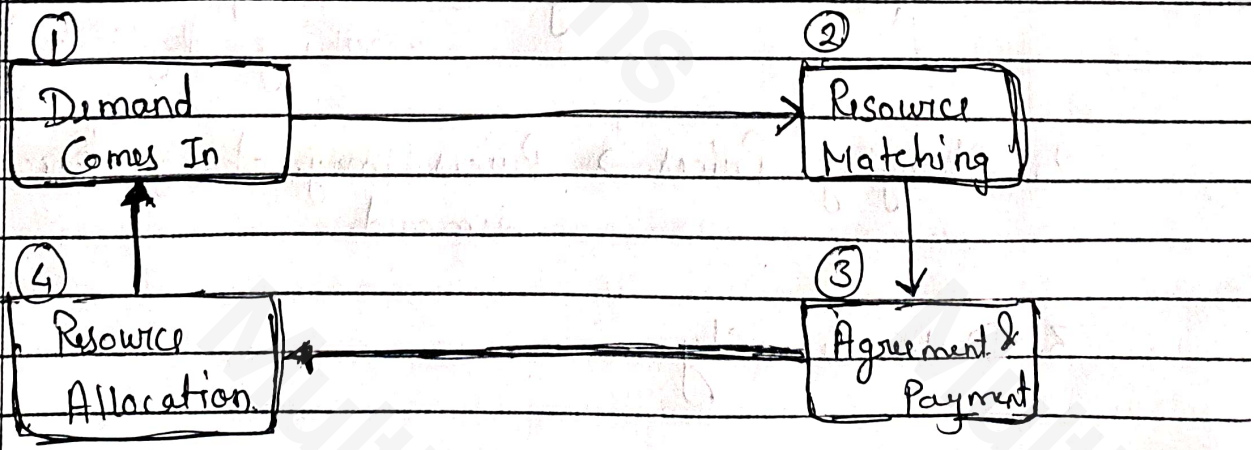
Page No.:
Date : / /

2. Key Players in the Marketplace

- Brokers : These are like middleman or agents who help customers find the right resources.
- Providers : They own the data centers & resources and make these available in the marketplace.
- Customers : They use resources. (pay per use model)

3. How it works

1. Demand Comes In : Companies need extra resources.
2. Resource Matching : The CEx checks the marketplace and finds a provider with enough resources available in the required region.
3. Agreement & Payment : A Service-Level Agreement (SLA) is created to guarantee the quality of service & payments are arranged securely.
4. Resource Allocation : Resources are assigned to the Compan



Page No.
Date: / /

Benefits of this Setup.

1. Flexible Scaling
2. Cost - Effective
3. Reliability

Simple Real-world Example

→ Imagine Company X has an app that suddenly becomes popular in Japan. Their main cloud provider only has a small data center in Japan & can't handle the sudden demand.

→ Through the Global Exchange, the provider borrows resources from another provider that has available capacity in Japan.

→ Company X's app stays online, and they pay only for the extra resources they used.

Challenges to Keep in Mind.

1. Complex Coordinating. [Multiple provider working together]
2. Changing Prices → Prices may change based on demand.
3. Data Security

Page No.:
Date : / /

Cloud Security Overview

→ Cloud Security is the set of practices, tools & procedures designed to protect cloud-based applications, data & infrastructure from both internal & External threats.

→ As organizations shift towards digital transformation, incorporating cloud-based solutions & services into their infrastructure, they face new Security challenges.

→ Cloud security helps them navigate these challenges to ensure the safety & integrity of their data & operations.

AKTU - 2021-22, 22-23 & 23-24

As cloud environments grow more complex and interconnected, these security challenges increase, requiring strong governance strategies to maintain control over security practices & compliance.

Security Challenges in Cloud Computing

1. **Data Breaches :** Cloud environments store large volume of sensitive data, making them attractive targets for cyber attackers.

Page No.
Date / /

2. **Data Loss**: Misconfigured storage, accidental deletion & hardware failures can lead to data loss in the cloud. without backup, organizations risk losing critical information.

3. **Lack of Visibility**: Cloud resources are often accessed outside the org.'s local network, making it hard for IT teams to monitor who is accessing, which can lead to unauthorized access.

4. **Multitenancy Risks**: In public clouds, resources are shared among multiple clients → making it possible for security issues.

5. **Access Management**: Managing access in a cloud environment is challenging, especially with employees using personal devices & accessing cloud services from various locations.

6. **Misconfiguration**: Many cloud security incidents occur due to misconfigured resources.

7. **Advanced Threats** & Insider Attacks.

→ DDOS [Distribution Denial of Service] attacks.
→ ransomware.
→ Insider threats.

Page No.:
Date : / /

Security Governance in Cloud Computing

→ Security governance involves establishing policies, procedures & standards to manage & protect cloud environments effectively.

1. **Policy Development**: Define & document clear security policies specific to cloud environments, covering data protection, access management, incident response, etc.

2. **Identity & Access Management (IAM)**: Implement IAM to control who has access to cloud resources and what they can do with those resources. This includes Multi-factor authentication, regular access reviews, etc.

3. **Data Protection & Encryption**: Develop policies for data encryption to protect sensitive information from unauthorized access. Ensure encryption keys are managed securely.

4. **Incident Response & Recovery**: Establish incident response plan that includes steps for detecting, containing & resolving security incidents.

5. **Training & Awareness**: Educate employees & stakeholders about cloud security best practices. Security awareness training reduces the risk of human errors and insider threats.

Page No.
Date / /

* Software as a Service (SaaS) Security

→ SaaS security focuss on securing applications delivered via the cloud, where users access software hosted by third-party providers over the internet.

→ With SaaS, providers manage the infrastructure, platform & software, but security responsibilities are often shared between the provider & the customer.

Importance

SaaS solutions offer organizations flexible, scalable, & easily accessible tools to enhance productivity.

Key SaaS Security Challenges:

1. Account Takeover
2. Data Loss
3. Phising
4. Denial of Service (DoS)

Page No.:
Date: / /

SaaS Security Best Practices

1. **Automated Discovery**: Continuously monitor to quickly detect & secure any unauthorized or unmanaged applications.

2. **User Education**: Train employees on security risks associated with SaaS applications.

3. **Strong Authentication**: Use multi-factor authenication

4. **Data Encryption**

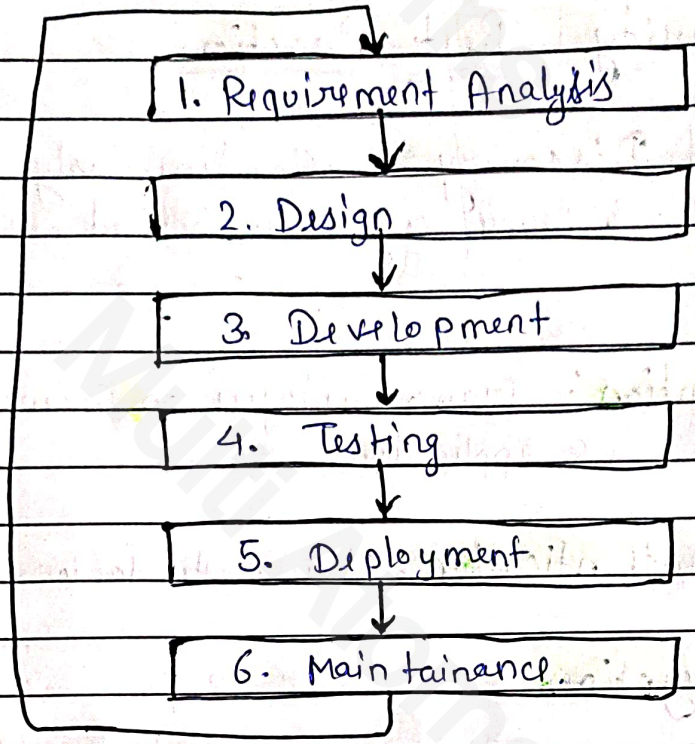
[AKTU - 2022-23]

Q. Describe the Secure Software Development life cycle with neat diagram.

→ ## Secure Software Development Life Cycle

The Secure SDLC is a process that incorporates security measures into each phase of the software development life cycle.

This helps in identifying & addressing security vulnerabilities as early as possible, reducing risks & costs associated with fixing security issues later in the process.



1. **Requirement Analysis**: Identify Security requirement based on business & technical needs

2. **Design**: Plan the software structure & define security controls. In this [identify potential vulnerabilities]

3. **Development**: Implement security best practices in coding

4. **Testing**: Perform various security testing [e.g vulnerability Scanning] to identify flaws before deployment.

5. **Deployment**: Ensuring secure deployment of the software. configurations applying to secure the environment.

Page No.:
Date : / /

6. **Maintainance** : Continuously monitor & update the software to handle new vulnerabilities. conduct regular audits, etc.

* What is Virtualized Security ?

→ also known as Security Virtualization

→ It refers to security solutions that are software-based & designed for virtualized IT environments.

→ Unlike traditional hardware-based security, which is static and tied to specific devices (like routers), virtualized security is flexible & dynamic, allowing it to be deployed anywhere in the network.

→ This flexibility is essential in cloud environments, because workloads & applications are created dynamically.

How Virtualized Security Works

Virtualized Security replicates the functions of tradional security appliances (e.g → firewalls & antiviruses) through software. It also leverages virtualization-specific security strategies.

- **Micro-Segmentation** Creating secure zones to limit attacker movement within the network.
- **Encryption** b/w application layers & infrastructure.

Benefits.	Risks.
1. Cost - Effectiveness	1. Complexity.
2. Flexibility	2. Workload management
3. Operational Efficiency	

Types of Virtualization Security

1. Segmentation :

Limits access to resources by controlling traffic between network segments.

2. Micro - Segmentation :

Applies specific policies to each workload, enhancing security within the data center. [rules to individual application]

3. Isolation :

Separates workloads & virtual networks, especially critical in multi-tenant public clouds to protect infrastructure.

Page No.:
Date: / /

Cloud IAM

→ Cloud Identity & Access Management refers to the processes, tools & policies that allow organizations to manage who has access to their cloud-based resources and applications.

→ It helps to control & moniter user's access to ensure that only authorized individuals or systems can perform specific tasks or access sensitive data within a cloud environment.

Key Components of Cloud IAM:

1. Resources [storage, processing power & analytics]
2. Permissions [Roles that defins who can access]
3. Roles [authorized users Roles]
4. Groups [A collection of users with similiar permissions]
5. Members [The actual users]

→ **Benefits:**

1. Security
2. Global Accessibility
3. Cost Effectiveness
4. Automation.

Page No.
Date / /

Best Practices for Cloud IAM:

1. Use Multi-factor Authentication.
2. Limit Admin Access
3. Monitor Continously.

* Cloud Security Standards

→ It provide a detailed framework that Organizations must follow to in order to Secure their cloud environments.

→ These standards focus on various aspects like privacy, data protection & secure configurations, offering clear roadmap for business to operating in the cloud.

Common Cloud Security Standards.

1. ISO Standards:

- ISO 27001: This Information security management standards offers a framework for managing information security risks & controls.
- ISO 27017: Upgrade version of ISO 27001

Page No.:
Date : / /

2. PCI DSS (Payment Card Industry Data Security standards)

→ Essential for businesses handling credit card data, PCI DSS ensures that cardholder information is processed, stored & transmitted securely

3. GDPR [General Data Protection Regulation]

→ Enforces strict data privacy & security standards for individuals in the Europe. Europe residents data must including data protection & transparency.

[AKTU - 2023-24]

4. NIST (National Institute of Standards & Technology [U.S. Security Guidelines]

It provides a guide to keeping data secure. Many U.S. businesses & agencies follow these guidelines to make sure they're doing things safely in the cloud.

5. CIS Controls:

→ The Center for Internet Security provides a list of best practices that companies can follow to improve security in the cloud.

6. SOC Reporting:

→ These Reports check if a company has the right security measures for data protection, especially for providers serving other businesses.

Page No.
Date / /

AKTU - 2021-22

Q. What is Honey pot? what are the difference types of Honey pot?

→

Honeypot

→ A Honeypot is a Cyber Security tool that acts like a trap for hackers.

→ It looks like a real part of a company's computer system, but it's actually fake & carefully monitored.

→ The goal is to attract hackers, who watch what they do & learn how they try to break in.

→ This helps security teams understand new threats, spot attackers early & keep them away from real systems.

Types of Honeypots

Based on why They're Used

1. Research Honeypots: Used to study hackers & learn their methods. These honeypots help security experts understand new attack techniques & create strong defenses.

Page No.:
Date : / /

2. **Production Honeypots:** Used by companies to catch real attackers, They protect actual systems by drawing attackers away from valuable data.

* **Based on How Much Interaction They Allow Hackers.**

1. **Low-Interaction Honeypots:** These pretend to be simple systems, like just a login page and can catch basic attacks

2. **Medium-Interaction Honeypots:** These offers more realistic but limited functions, like part of a server. They can show more details about what the hacker is trying to do.

3. **High-Interaction Honeypots:** These are very detailed and act like real systems, allowing hackers to explore more.

They reveal alot about hacker methods but must be closely watched to ensure the hacker doesn't use them to harm other systems.

Unit-4 Completed Subscribe

MULTI ATOMS