REGULATION- 2023

TC-04, W.e.f: 01.06.2024
Format Number: 21 Ver: 1.0

DEPARTMENT of CSE

SUBJECT CODE: 23CSX507 **SEM: VI**
SUBJECT NAME: Cloud Computing and Virtualization **YEAR: III**

UNIT-I INTRODUCTION TO CLOUD COMPUTING

Introduction to Cloud Computing: Overview, Roots of Cloud Computing, Layers and Types of Cloud, Desired Features of a Cloud, Benefits and Disadvantages of Cloud Computing, Cloud Infrastructure Management, Infrastructure as a Service Providers, Platform as a Service Providers, Challenges and Risks, Assessing the role of Open Standards.

1.Analyze the differences among IaaS, PaaS, and SaaS. (K4)

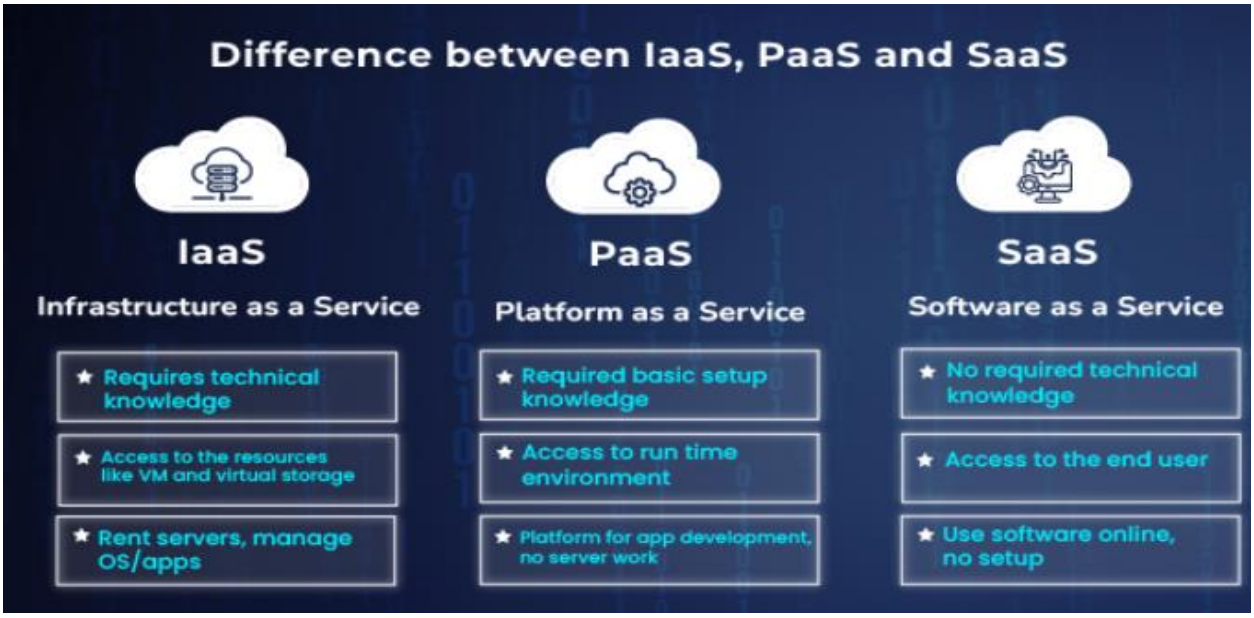
Cloud computing service models differ mainly in the level of abstraction**,** user control**,** and responsibility sharing between the cloud provider and the user.

Infrastructure as a Service (IaaS) offers the lowest level of abstraction by providing virtualized hardware resources such as servers, storage, and networking. Users have maximum control over the operating systems, applications, and data, making IaaS suitable for organizations that need flexibility and customization but are willing to manage security and maintenance at the software level.

Platform as a Service (PaaS) provides a higher level of abstraction by offering a ready-to-use development platform. The cloud provider manages the infrastructure, operating system, and runtime environment, while users focus only on application development and data. This model reduces development complexity and time but limits control over the underlying infrastructure.

Software as a Service (SaaS) delivers fully functional applications over the Internet with the highest level of abstraction. The provider manages the entire stack, including infrastructure,

platform, and software, while users simply access the application through a browser. SaaS offers ease of use and minimal maintenance but provides the least customization and control.



Aspect	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
Definition	Provides virtualized computing infrastructure over the Internet	Provides a platform with tools to develop, test, and deploy applications	Provides ready-to-use software applications over the Internet
User Control	High control over OS, storage, and applications	Control over applications and data only	Minimal control; user only uses the software
Managed by Provider	Physical servers, networking, virtualization	Infrastructure, OS, runtime, middleware	Entire stack including application
User Responsibility	OS, middleware, runtime, applications, data	Applications and data	Only data and user settings
Target Users	System administrators, IT teams	Application developers	End users
Scalability	Highly scalable	Highly scalable	Automatically scalable
Cost Model	Pay per use of infrastructure	Pay per use of platform services	Subscription or usage-based
Examples	AWS EC2, Google Compute Engine, Azure VM	Google App Engine, Azure App Service, Heroku	Gmail, Google Docs, Salesforce

2.Evaluate the suitability of public, private, and hybrid clouds for healthcare systems.

Healthcare systems are among the most data-intensive and sensitive domains, dealing with patient health records, diagnostic images, laboratory reports, billing data, and real-time clinical systems**.** These systems must ensure data privacy, security, availability, scalability, and compliance with healthcare regulations such as HIPAA, GDPR, and national health data protection laws. Cloud computing offers powerful solutions, but the choice of cloud deployment model-public, private, or hybrid-significantly impacts healthcare operations.

Public Cloud for Healthcare Systems

Concept and Architecture

A public cloud is owned and operated by third-party cloud providers such as AWS, Microsoft Azure, or Google Cloud. The infrastructure is shared among multiple organizations, and services are accessed over the Internet using a pay-as-you-use model.

Evaluation in Healthcare

Public clouds provide high scalability and cost efficiency but offer limited control over infrastructure. In healthcare, this makes them suitable mainly for non-critical and non-confidential workloads rather than core clinical systems.

Advantages in Healthcare

- **Cost efficiency**: No capital investment in servers or data centers.
- **Elastic scalability**: Useful during peak demands such as pandemics or mass screenings.
- **Rapid deployment**: New healthcare applications can be launched quickly.
- **Advanced analytics and AI**: Supports large-scale medical data processing.

Limitations in Healthcare

- Data privacy concerns due to multi-tenant architecture.
- Regulatory compliance challenges for sensitive patient data.
- Limited customization and control over security policies.
- Dependence on reliable Internet connectivity.

Real-World Healthcare Applications

- Telemedicine platforms hosting video consultations.

- Public health dashboards for disease surveillance.
- Medical research platforms analyzing anonymized datasets.
- Patient appointment systems and portals.

Overall Suitability

Public cloud is moderately suitable for healthcare when used for supporting services, research, and analytics, but not ideal for storing or processing sensitive patient data.

2. Private Cloud for Healthcare Systems

Concept and Architecture

A **private cloud** is dedicated to a single healthcare organization and can be hosted on-premises or managed by a third party. The infrastructure is **not shared**, providing greater control and security.

Evaluation in Healthcare

Private clouds are well suited for healthcare organizations that must maintain strict confidentiality , compliance, and operational control.

Advantages in Healthcare

- High security and data privacy, essential for patient records.
- Full control over infrastructure and access policies.
- Easier compliance with healthcare regulations.
- Customizable to meet hospital-specific workflows.

Limitations in Healthcare

- High initial and operational costs.
- Requires skilled IT professionals.
- Limited scalability compared to public cloud.
- Maintenance responsibility lies with the organization.

Real-World Healthcare Applications

- Electronic Health Records (EHR) systems.
- Hospital Information Systems (HIS).
- Picture Archiving and Communication Systems (PACS) for medical imaging.
- National or government healthcare databases.

Overall Suitability

Private cloud is **highly suitable** for healthcare organizations where **security, privacy, and compliance** are top priorities.

3. Hybrid Cloud for Healthcare Systems

Concept and Architecture

A hybrid cloud integrates both public and private cloud environments, allowing data and applications to move securely between them.

Evaluation in Healthcare

Hybrid cloud provides the optimal balance between security and scalability, making it the most preferred model for modern healthcare systems.

Advantages in Healthcare

- Sensitive patient data remains in the private cloud.
- Public cloud used for analytics, AI diagnostics, and telemedicine.
- Cost-effective compared to full private cloud.
- Strong support for disaster recovery and business continuity.
- Enables innovation without compromising data security.

Limitations in Healthcare

- Complex architecture and management.
- Requires robust security integration and governance.
- Higher implementation complexity.

Real-World Healthcare Applications

- EHR stored in private cloud, AI-based diagnosis in public cloud.
- Medical research using anonymized data in public cloud.
- Disaster recovery systems using public cloud storage.
- National digital health platforms combining both models.

3.**Design a cloud infrastructure management plan for a medium-sized enterprise.**

Introduction

A medium-sized enterprise (MSE) requires a cloud infrastructure that is scalable, secure, cost-effective, and highly available to support business applications, data storage, and user access. A cloud infrastructure management plan defines how cloud resources are designed, deployed, monitored, secured, and optimized to meet business goals.

Objectives of the Cloud Infrastructure Plan

- Ensure high availability and reliability
- Support scalability and performance
- Maintain data security and compliance
- Optimize cost and resource utilization
- Enable easy management and monitoring
- Provide disaster recovery and business continuity

Cloud Deployment Model

For a medium-sized enterprise, a Hybrid Cloud Model is most suitable.

- **Public Cloud**: For web applications, development, testing, and non-critical workloads
- **Private Cloud**: For sensitive data, internal applications, and compliance-related workloads

Benefits:

- Flexibility and scalability
- Cost optimization
- Better security control for critical data

Cloud Service Model Selection

The enterprise will use a combination of:

1. **Infrastructure as a Service (IaaS)**
   - Virtual machines, storage, networking
   - Example: AWS EC2, Azure Virtual Machines
2. **Platform as a Service (PaaS)**
   - Application development and deployment
   - Example: Google App Engine, Azure App Services
3. **Software as a Service (SaaS)**
   - Business applications like email, CRM
   - Example: Microsoft 365, Salesforce

Infrastructure Architecture Design

- **Compute Resources**: Auto-scaling virtual machines and containers
- **Storage**:
  - Object storage for backups and media

  - Block storage for databases
  - File storage for shared access
- **Networking**:
  - Virtual Private Cloud (VPC)
  - Load balancers
  - Secure VPN and firewall rules

Resource Provisioning and Configuration

- Use **Infrastructure as Code (IaC)** tools like Terraform or ARM templates
- Standardize VM images and configurations
- Automate provisioning to reduce errors and deployment time

Security and Compliance Management

Security is a critical part of cloud infrastructure management.

- **Identity and Access Management (IAM)**:
  - Role-based access control
  - Multi-factor authentication (MFA)
- **Data Security**:
  - Data encryption at rest and in transit
- **Network Security**:
  - Firewalls, security groups, intrusion detection
- **Compliance**:
  - Follow standards like ISO 27001, GDPR, HIPAA

Monitoring and Performance Management

- Use cloud monitoring tools such as:
  - AWS CloudWatch
  - Azure Monitor
- Monitor:
  - CPU, memory, disk usage
  - Network latency
  - Application availability
- Configure alerts for threshold breaches

Cost Management and Optimization

- Use **pay-as-you-go pricing**
- Implement:
  - Resource tagging
  - Budget alerts
  - Reserved instances for long-term workloads

- Regularly review unused or underutilized resources

Backup, Disaster Recovery, and Business Continuity

- Regular automated backups
- Multi-region data replication
- Disaster Recovery (DR) strategy:
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
- Periodic DR drills and testing

4.Examine how different PaaS services support enterprise application deployment. (k4)

Platform as a Service (PaaS) provides a complete cloud-based environment for developing, deploying, managing, and scaling enterprise applications. Different PaaS providers support enterprise application deployment in varied ways, depending on their architecture, tools, and integrations.

1. Google App Engine (GAE)

- Fully managed platform with automatic scaling.
- Supports multiple programming languages (Java, Python, Go, PHP, Node.js).
- Built-in services for load balancing, monitoring, and logging.
- Strong integration with Google Cloud services (BigQuery, Cloud SQL).
- Ideal for enterprises needing rapid deployment with minimal infrastructure management.

2. Microsoft Azure App Service

- Supports .NET, Java, Python, Node.js, and PHP.
- Seamless integration with Microsoft enterprise tools (Active Directory, Office 365).
- CI/CD support through Azure DevOps and GitHub.
- High availability with auto-scaling and load balancing.
- Strong security and compliance features.

3. AWS Elastic Beanstalk

- Simplifies application deployment without managing infrastructure.
- Supports Java, .NET, PHP, Python, Ruby, Node.js, and Docker.
- Automatic handling of capacity provisioning, load balancing, and monitoring.
- Integrates with AWS services like RDS, S3, and CloudWatch.

4. Red Hat OpenShift

- Kubernetes-based enterprise PaaS.
- Supports containerized applications and microservices.
- Strong DevOps and CI/CD pipeline integration.
- Hybrid and multi-cloud support.
- Enterprise-grade security and compliance

5. Salesforce Platform (Force.com)

- Low-code/no-code development capabilities.
- Built-in CRM and business process integration.
- High availability and automatic upgrades.
- Strong data security and role-based access control

6. Oracle Cloud PaaS

- Optimized for enterprise databases and middleware.
- Strong support for Java EE, Oracle DB, and enterprise integration patterns.
- Built-in security, compliance, and identity management