माधव प्रौद्योगिकी एवं विज्ञान संस्थान, ग्वालियर (म.प्र.), भारत

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR (M.P.), INDIA

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Government of India)

NAAC ACCREDITED WITH A++ GRADE

PROFICIENCY ON CLOUD COMPUTING (3160515)

Presented to
Prof. Kumud Dixit

Presented by
Prathmesh Deshkar
(0901IT243D04)

Understanding Cloud Infrastructure and Delivery Models

Cloud computing has revolutionized how organizations design, deploy, and manage their IT infrastructure. This comprehensive exploration covers the fundamental architecture models, delivery frameworks, virtualization techniques, security considerations, and programming paradigms that define modern cloud environments.

Infrastructure Models

Explore public, private, hybrid, and community cloud architectures that form the foundation of cloud computing ecosystems.

Virtualization Concepts

Understand how virtualization maximizes resource utilization and enables flexible, scalable computing environments.

Security & Programming

Master security frameworks and programming models essential for building robust, enterprise-grade cloud solutions.

Cloud Infrastructure Models: Public, Private, Hybrid, Community

Organizations select infrastructure models based on control requirements, security needs, compliance obligations, and cost considerations. Each model offers distinct advantages for different business scenarios.

Public Cloud

Shared multi-tenant resources accessible to any customer via the internet, offering maximum scalability and cost efficiency.

- Examples: AWS, Azure, Google Cloud
- Pay-as-you-go pricing model
- Rapid deployment and elasticity

Private Cloud

Dedicated infrastructure exclusively for one organization, providing enhanced control, security, and customization capabilities.

- On-premises or hosted options
- Complete data sovereignty
- Tailored security policies

Hybrid Cloud

Seamlessly combines public and private clouds, enabling workload portability and optimized resource allocation across environments.

- Flexibility for varying workloads
- Balance cost and control
- Cloud bursting capabilities

Community Cloud

Shared infrastructure serving organizations with common compliance, security, or industry-specific requirements.

- Healthcare, government sectors
- Shared compliance costs
- Collaborative governance

Cloud Delivery Models: IaaS, PaaS, SaaS

Cloud service models represent different levels of abstraction and responsibility sharing between providers and customers. Understanding these distinctions is crucial for selecting appropriate solutions.

IaaS: Infrastructure as a Service

Provides virtualized computing resources including servers, storage, and networking on demand. Users manage operating systems, middleware, and applications while providers handle physical infrastructure.

Examples: AWS EC2, Azure Virtual Machines

Use case: Custom environments, full control

Responsibility: High user management

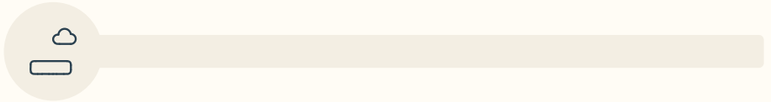
PaaS: Platform as a Service

Delivers complete development and deployment platforms with integrated tools, middleware, and runtime environments. Developers focus on code while providers manage underlying infrastructure and platforms.

Examples: Google App Engine, Heroku

Use case: Application development, DevOps

Responsibility: Shared management model



SaaS: Software as a Service

Offers ready-to-use applications accessed via web browsers or APIs. Providers manage everything from infrastructure to application updates, while users simply consume the software.

Examples: Microsoft 365, Salesforce

Use case: Business applications, collaboration

Responsibility: Minimal user management

Virtualization Concepts & Security in Cloud Computing

Virtualization Fundamentals

Virtualization technology creates abstract layers between physical hardware and operating systems, enabling multiple isolated virtual machines (VMs) to run simultaneously on single physical servers. This breakthrough maximizes resource utilization, reduces hardware costs, and provides unprecedented flexibility.

Hypervisors: Type 1 (bare-metal) and Type 2 (hosted) virtualization managers

Resource pooling: Dynamic allocation of CPU, memory, and storage

Isolation: Secure separation between virtual environments

Snapshot capabilities: Instant backup and recovery mechanisms

Security Virtualization Challenges

While virtualization offers isolation benefits, shared physical resources introduce unique security risks requiring specialized protection strategies.

VM Escape Attacks

Malicious code breaking out of virtual machine boundaries to access hypervisor or other VMs

Hypervisor Vulnerabilities

Exploits targeting the virtualization layer itself, affecting all hosted virtual machines

Resource Contention

Performance degradation and side-channel attacks through shared hardware resources

Choosing Programming Models & Public Cloud Platforms

Selecting the optimal programming paradigm and cloud platform requires careful analysis of workload characteristics, performance requirements, development team expertise, and long-term scalability needs.

Serverless Computing

Containerized Microservices

Traditional Virtual Machines

Leading Public Cloud Platforms

Amazon Web Services

Market leader with a vast service catalog, advanced AI/ML tools, global reach, and strong enterprise support.

Best for: Startups, web applications, serverless architectures, and organizations prioritizing service breadth and innovation.

Microsoft Azure

Deep Microsoft ecosystem integration, powerful hybrid cloud features, strong compliance, and seamless Active Directory support.

Best for: Enterprises with existing Microsoft investments, hybrid deployments, and organizations requiring government compliance.

Google Cloud Platform

Excellent data analytics and ML services, top-tier Kubernetes support, competitive pricing, and advanced BigQuery features.

Best for: Data-intensive applications, machine learning projects, and organizations prioritizing analytics and containerization.

Composing Cloud Solutions: Integrating Virtualization, Security & Programming

Building production-ready cloud applications requires orchestrating multiple technical domains into cohesive, secure, and maintainable architectures that align with business objectives.

01

Virtualization Strategy

Create resource allocation policies, harden hypervisors, manage VM lifecycles, and set up network segmentation for better performance and isolation.

02

Layered Security Framework

Implement Zero Trust with identity checks, use end-to-end encryption, set strong IAM policies, and enable continuous security monitoring.

03

Programming Model Selection

Evaluate workload characteristics against serverless, containerized, and VM-based approaches. Consider development velocity, operational complexity, and cost optimization.

04

Platform Integration

Leverage cloud-native services like managed databases, message queues, and AI/ML APIs. Implement infrastructure as code for reproducible deployments and version control.

05

Shared Responsibility Model

Clearly define security boundaries between cloud provider and customer responsibilities. Implement compliance controls, audit logging, and incident response procedures.