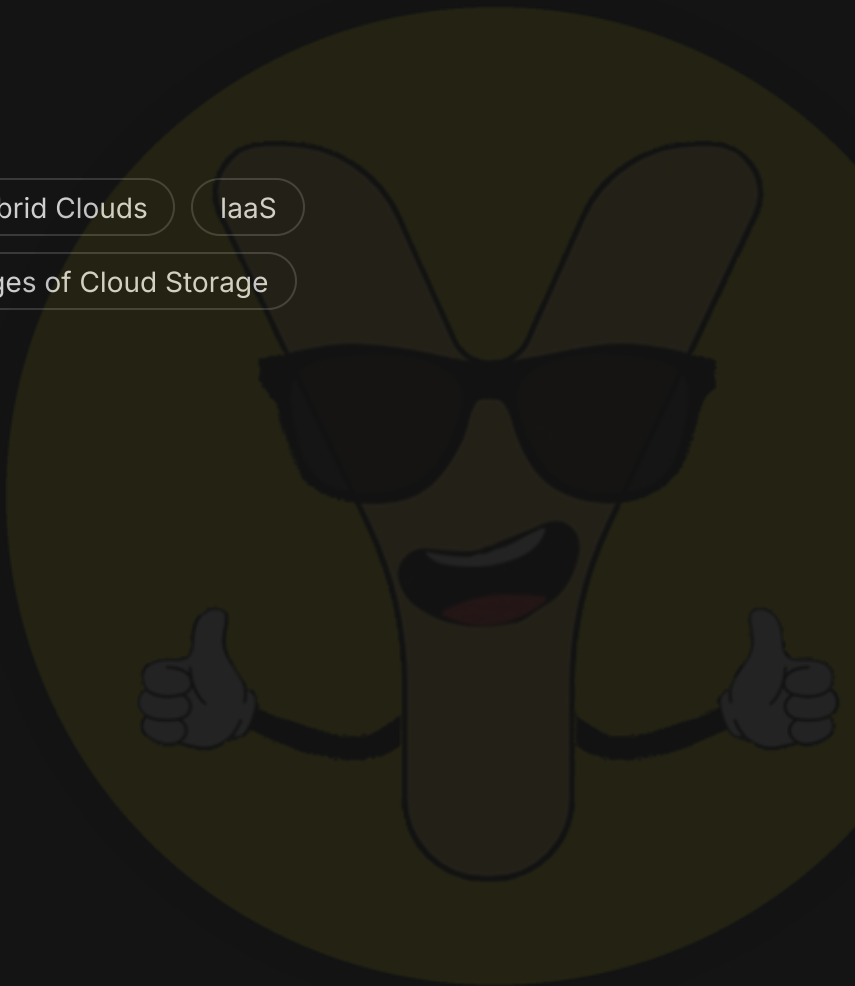
AKTU · 3RD YEAR · SEMESTER 5 · BCAM051

Cloud Computing

Unit 3 — Cloud Architecture, Services and Storage

- Layered Cloud Architecture Design
- NIST Cloud Computing Reference Architecture
- Public, Private and Hybrid Clouds
- IaaS
- PaaS
- SaaS
- Architectural Design Challenges
- Cloud Storage
- Storage-as-a-Service
- Advantages of Cloud Storage
- Cloud Storage Providers
- S3

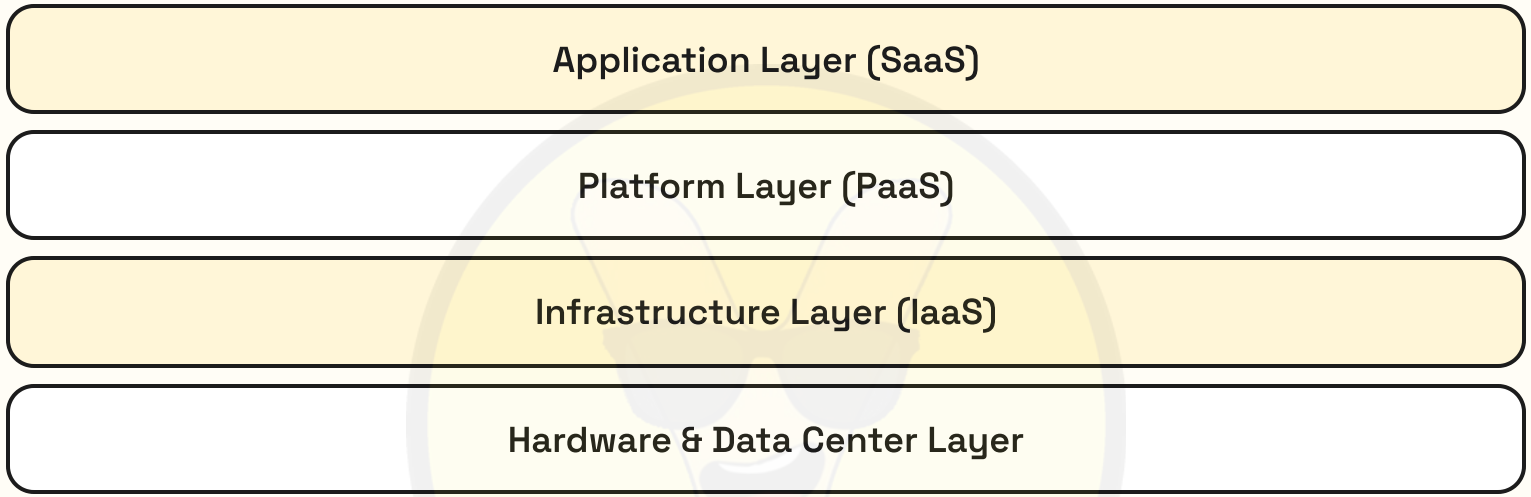


DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Layered Cloud Architecture Overview



4-Tier Layered Cloud Architecture Model

Layered Cloud Architecture Design

Cloud architecture is structured into hierarchical layers, where lower abstraction layers provide services to higher layers.

- Application Layer (SaaS)
  - Houses user-facing applications like web portals, CRM, and email.
  - Maintained entirely by cloud service providers without user infrastructure management.
- Platform Layer (PaaS)
  - Provides application execution frameworks, database management, and runtime environments.
  - Hides underlying virtual machines and hardware complexity from software developers.
- Infrastructure Layer (IaaS)
  - Manages virtualized compute, storage, and networking resources.
  - Uses hypervisors to dynamically allocate physical hardware to virtual instances.
- Hardware Layer
  - Consists of physical servers, SAN/NAS storage, routers, switches, and cooling systems.
  - Forms the backbone located in geographically distributed data centers.

NIST Cloud Computing Reference Architecture



NIST SP 500-292 Reference Model Actor Roles

NIST Reference Architecture Roles

NIST SP 500-292 defines a standard conceptual model identifying five major actors in cloud computing.

- Cloud Consumer
  - Person or organization that maintains a business relationship with, and uses service from, Cloud Providers.
- Cloud Provider
  - Entity responsible for making a cloud service available to interested consumers.
- Cloud Auditor
  - Independent party that conducts unbiased assessments of cloud services, security, privacy, and performance.
- Cloud Broker
  - Entity that manages the use, performance, and delivery of cloud services, negotiating relationships between providers and consumers.
- Cloud Carrier
  - An intermediary that provides connectivity and transport of cloud services between Cloud Consumers and Cloud Providers.

Public, Private, and Hybrid Cloud Deployment Models

Parameter	Public Cloud	Private Cloud	Hybrid Cloud
Ownership	Third-party cloud provider	Single enterprise / Organization	Shared between internal & public provider
Access & Multi-tenancy	Multi-tenant; open to general public	Single-tenant; restricted internal access	Mixed multi-tenant and single-tenant
Cost Model	Pay-as-you-go; low initial CapEx	High initial CapEx; predictable OpEx	Balanced CapEx and flexible OpEx
Security & Control	Lower control; vendor managed	Maximum control & strict data governance	High security for sensitive data; flexible for general workloads
Scalability	Near infinite, instant elasticity	Limited by physical datacenter capacity	Dynamic bursting to public cloud (Cloud Bursting)
Use Cases	Web applications, public APIs	Financial systems, Healthcare records	E-commerce seasonal spikes, disaster recovery

Infrastructure as a Service (IaaS)

IAAS

IaaS is a cloud service model where consumers rent automated, highly scalable computing resources including virtual machines, block storage, firewalls, and networks on a pay-per-use basis.

- Consumer controls operating systems, deployed applications, storage, and networking components (e.g., host firewalls).
- Provider manages physical hardware, virtualization layer (hypervisor), data centers, and physical networking.
- Key Examples: Amazon EC2, Google Compute Engine (GCE), Microsoft Azure VMs.
- Pricing is typically billed per second or hour based on allocated virtual CPUs (vCPUs) and RAM.

Platform as a Service (PaaS)

PAAS

PaaS provides a cloud-hosted development and deployment framework, including operating systems, programming language runtimes, libraries, services, and database management systems.

- Developers focus purely on application code and business logic without managing underlying VMs or OS patching.
- Provider manages underlying OS, middleware, runtime environments, hardware infrastructure, and hypervisors.
- Includes built-in automatic scaling, load balancing, and integrated developer tooling.
- Key Examples: AWS Elastic Beanstalk, Google App Engine, Heroku.

Software as a Service (SaaS)

SAAS

SaaS is a software distribution model in which applications are hosted by a cloud service provider and made available to end-users over the internet via a web browser or lightweight API interface.

- End-users do not manage or control the underlying cloud infrastructure, operating systems, or application code.
- Minimal client-side installation required; software updates and security patches are automatically applied by the provider.
- Operates on a subscription-based licensing model or tier-based user billing.
- Key Examples: Google Workspace, Salesforce, Microsoft 365, Dropbox.

Comparative Summary: IaaS vs PaaS vs SaaS

Feature	IaaS	PaaS	SaaS
Primary Target Audience	System Administrators & IT Infra Teams	Software Developers & DevOps	End-Users & Enterprise Business Units
Managed by Consumer	OS, Runtime, Data, Application, Middleware	Application Code and Data only	Application Configurations & User Data only
Managed by Provider	Virtualization, Servers, Storage, Networking	OS, Runtime, Middleware, Infra	Entire Stack (Application to Hardware)
Flexibility & Control	Highest technical control and customization	Moderate control over runtime/config	Lowest technical flexibility
Ease of Deployment	Requires manual OS setup & administration	Requires coding & packaging	Immediate access via browser / API
Unit of Scale	Virtual Machines / Instances	Applications / Services	Users / Seats / Subscription

Architectural Design Challenges in Cloud Computing

Designing robust, secure, and performant cloud architectures involves resolving complex system engineering trade-offs.

- Data Lock-in & Interoperability
  - Proprietary APIs prevent easy migration of applications between distinct cloud providers.
  - Lack of standardized cloud interfaces leads to high switching costs.
- Multitenancy & Resource Isolation
  - Ensuring strong logical separation between multiple tenants sharing physical hardware.
  - Mitigating side-channel security attacks and noisy neighbor issues.
- Data Security & Privacy
  - Protecting sensitive data at rest and in transit using end-to-end encryption.
  - Compliance with strict regulatory frameworks like GDPR, HIPAA, and PCI-DSS.
- Scalability & Latency
  - Managing horizontal autoscaling latency during unexpected traffic spikes.
  - Minimizing network latency across geographically distributed regions.
- SLA & Availability
  - Achieving high availability (e.g., 99.999% uptime) despite physical hardware failures.

Cloud Storage Request Flow



Execution Path of Data Access Request in Cloud Storage Architecture

Storage-as-a-Service (STaaS)

STORAGE-AS-A-SERVICE (STAAS)

STaaS is an architectural model where an enterprise or consumer leases virtualized cloud storage capacity from a provider on a subscription or pay-per-gigabyte basis.

- Provides raw block storage, file storage, or object storage accessible over network protocols (HTTP/REST, NFS, iSCSI).
- Eliminates high upfront Capital Expenditure (CapEx) for physical Storage Area Networks (SAN) or Network-Attached Storage (NAS).
- Includes features like automated snapshot backups, geo-replication, deduplication, and data compression.
- Reduces operational overhead by outsourcing disk replacement and array maintenance to the provider.

Key Advantages of Cloud Storage

Cloud storage offers substantial technical and financial benefits over traditional local storage devices.

- Elasticity & Unlimited Capacity
  - Storage scales dynamically on-demand without manual disk provisioning or physical installation.
- Cost-Efficiency
  - Shifts costs from CapEx to OpEx; users pay only for the exact gigabytes consumed.
- High Durability & Availability
  - Data is automatically replicated across multiple availability zones and physical drives.
  - Achieves high durability figures (e.g., 99.999999999% or 11 9s in AWS S3).
- Accessibility & Mobility
  - Files can be securely accessed globally over standard HTTP/HTTPS REST APIs anytime.
- Automated Backup & Disaster Recovery
  - Built-in snapshot retention policies simplify backup automation and rapid data recovery.

Cloud Storage Providers & Storage Types

Cloud storage is categorized into three main types supported by major hyper-scaler vendors.

- Object Storage
  - Stores data as un-structured objects with metadata and a unique ID (e.g., AWS S3, Google Cloud Storage, Azure Blob).
  - Ideal for unstructured data like media, backups, and static web content.
- Block Storage
  - Splits data into fixed blocks acting as virtual raw hard drives (e.g., AWS EBS, Azure Managed Disks).
  - Ideal for databases (MySQL, Oracle) requiring high IOPS and low latency.
- File Storage
  - Organizes data into a hierarchical file folder structure (e.g., AWS EFS, Azure Files, GCP Filestore).
  - Shared access via standard protocols like NFS and SMB.
- Leading Providers
  - Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud.

Amazon Simple Storage Service (S3): Core Architecture

AWS S3 is an industry-standard object storage service offering scalable performance, data availability, and security.

- **Buckets**
  - Top-level container for storing objects; must have a globally unique name across all AWS accounts.
- **Objects**
  - Fundamental entity stored in S3, consisting of Object Data (payload), Key (unique name string), and Metadata.
- **Keys**
  - Unique identifier assigned to an object within a bucket (e.g., `images/photo.png`).
- **Storage Classes**
  - Standard (frequent access), Standard-IA (infrequent access), S3 Glacier (archival), Glacier Deep Archive.
- **Consistency Model**
  - Offers strong read-after-write consistency for PUT and DELETE requests of objects in all AWS regions.

Worked Example: S3 Storage Cost & Lifecycle Analysis

An organization uploads $500\ \text{GB}$ of logs monthly. For the first month, logs are in S3 Standard at $\$0.023/\text{GB}$. In month 2, lifecycle policies move them to S3 Standard-IA at $\$0.0125/\text{GB}$. In month 3, they move to Glacier Deep Archive at $\$0.00099/\text{GB}$. Calculate total storage cost over 3 months.

1. Month 1 Cost (S3 Standard): $500\ \text{GB} \times \$0.023 = \$11.50$
2. Month 2 Cost (S3 Standard-IA): $500\ \text{GB} \times \$0.0125 = \$6.25$
3. Month 3 Cost (Glacier Deep Archive): $500\ \text{GB} \times \$0.00099 = \$0.495$
4. Total Cumulative Cost over 3 months: $\$11.50 + \$6.25 + \$0.495 = \$18.245$

Total storage cost for hosting 500 GB of data over the 3-month tiered lifecycle is $18.25.

AKTU Exam Corner: Unit 3 Practice Questions

Q1 1. Explain the 4-layer Cloud Architecture Model in detail. Distinguish between physical and virtualized resources. (10 Marks)

Q2 2. Describe the NIST Cloud Computing Reference Architecture. Explain the roles of Cloud Broker, Cloud Auditor, and Cloud Carrier. (10 Marks)

Q3 3. Compare Public, Private, and Hybrid Cloud deployment models based on cost, security, scalability, and control. (7 Marks)

Q4 4. Differentiate between IaaS, PaaS, and SaaS with suitable real-world examples and management responsibility models. (10 Marks)

Q5 5. What are the key architectural design challenges in cloud computing? Discuss data lock-in and multitenancy isolation. (7 Marks)

Q6 6. Define Storage-as-a-Service (STaaS). Explain the structural differences between Block, File, and Object storage. (7 Marks)

Q7 7. Write a short note on Amazon S3 architecture. Explain S3 buckets, keys, object metadata, and storage classes. (7 Marks)

Unit 3 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 4 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

