UNIT–3 : Cloud Architecture, Services and Storage (PYQ Solution)

AKTU · Cloud Computing (BCAM051) · Solutions by **Chirag Jain**, Ycotes

SECTION A Answers (≈70 Words Each)

Q1. What is Service Oriented Architecture (SOA) and why is it important in cloud services? (Jan 2026)

SOA is an architectural style that builds applications from loosely coupled, reusable services with standard interfaces, communicating over a network using SOAP or REST. It is important in cloud services because cloud resources and applications are exposed as services through APIs. SOA brings interoperability, reuse, easy integration, independent scaling and faster development.

Q2. Define IaaS with one practical example from industry. (Jan 2026)

Infrastructure as a Service (IaaS) provides virtualized computing infrastructure such as virtual machines, storage and networks on a pay-per-use basis. The user manages the OS, middleware and applications; the provider manages the physical hardware. Example: Amazon EC2 is used by Netflix to run streaming and encoding workloads that scale up and down with demand.

Q3. Describe the features and benefits of IaaS, PaaS and SaaS. (Jan

2025)

Model	Features	Benefits
IaaS	Virtual servers, storage, networks; user controls OS	Flexibility, no hardware cost, scalable (EC2)
PaaS	Runtime, database, middleware, development tools	Faster development, automatic scaling, no infrastructure management (App Engine)
SaaS	Complete applications via browser	No installation, automatic updates, low cost, anywhere access (Gmail)

Q4. Explain Storage-as-a-Service. (Jan 2025)

Storage as a Service (STaaS) is a cloud model where providers rent storage capacity over the Internet for backup, archiving, file sharing and application data, billed per GB used. Examples: Amazon S3, Google Drive, Dropbox. Benefits: no storage hardware, elastic capacity, built-in replication and durability, remote access and disaster recovery. Risks: bandwidth dependence and data privacy.

Q5. Define community cloud with example. (2024)

A community cloud is infrastructure shared by several organisations with common concerns (mission, security, compliance or policy) and managed by them or a third party. It costs less than a private cloud but offers more control than a public cloud. Example: a government or healthcare community cloud shared by hospitals, or the cloud used jointly by several universities for research.

Q6. List the types of services provided by cloud. (2024)

- **IaaS (Infrastructure as a Service)**
- **PaaS (Platform as a Service)**
- **SaaS (Software as a Service)**
- **STaaS (Storage as a Service)**
- **DaaS (Database / Desktop as a Service)**
- **FaaS (Function as a Service, serverless)**

- **XaaS (Anything as a Service), e.g. Security as a Service and Backup as a Service.**

Q7. Illustrate the role of hypervisor in virtualization. (Feb 2024)

A hypervisor (virtual machine monitor) is software that creates and runs virtual machines on physical hardware. It allocates CPU, memory, storage and network to each VM, isolates the VMs from one another, schedules vCPUs on physical cores and mediates access to devices. Type 1 (bare-metal) hypervisors such as Xen and ESXi run directly on hardware; Type 2 (hosted) such as VirtualBox run on a host OS. It enables consolidation, migration and snapshots.

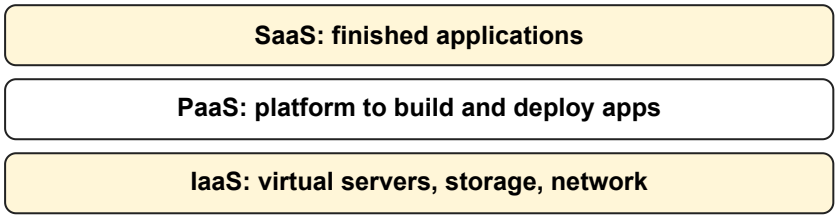
Q8. Discuss the advantages of cloud storage over traditional on-premises storage. (Feb 2024)

- **Lower cost: no up-front hardware; pay per GB.**
- **Scalability and elasticity: capacity grows or shrinks instantly.**
- **Accessibility: data reachable from anywhere on any device.**
- **Durability and availability: automatic replication and backups.**
- **Reduced maintenance: the provider handles hardware, patches and upgrades.**
- **Disaster recovery and easy collaboration.**
  Disadvantages: Internet dependence and data privacy concerns.

SECTION B Answers (≈250 Words Each)

Q1. Explain SaaS, PaaS and IaaS with suitable use-case based examples. (Jan 2026)

Cloud service models differ in how much the user manages.



Cloud service stack

- **IaaS:** raw infrastructure. The customer chooses the OS and installs software. **Use case:** a start-up hosts its web servers and database on **Amazon EC2** and scales VMs for a sale season. Customer controls OS, storage and apps; the provider controls hardware and virtualization.
- **PaaS:** a ready runtime and tools for building applications. **Use case:** a college develops its admission portal on **Google App Engine** or **Heroku**, writing only code while the platform handles servers, scaling and patches.
- **SaaS:** the provider delivers the complete software. **Use case:** a business uses **Gmail, Zoho CRM or Microsoft 365** through a browser with no installation or maintenance.

Model	User manages	Provider manages	Example
IaaS	OS, runtime, apps, data	Hardware, virtualization	EC2, Azure VM
PaaS	Apps, data	Everything below the app	App Engine, Heroku
SaaS	Only usage and settings	Everything	Gmail, Salesforce

Conclusion: choose IaaS for control, PaaS for developer speed and SaaS for ready-made functionality.

Q2. Discuss architectural design challenges in cloud environments. Analyze the trade-offs between performance and security with numerical examples. (Jan 2025)

Design challenges:

- **Service availability and reliability** (single points of failure, SLA).
- **Data privacy, security and compliance.**
- **Performance and latency** over the Internet.
- **Scalability and elasticity** of design.
- **Data lock-in, portability and interoperability.**
- **Resource management, multi-tenancy isolation** and billing/metering.
- **Legacy application migration.**

Performance versus security trade-off: stronger security adds processing and network overhead.

Example: an application serves a request in **100 ms** at **1,000 requests/s**.

- Add TLS and AES encryption (+20% time): latency = 100 × 1.2 = **120 ms**; throughput falls to 1,000/1.2 ≈ **833 req/s**.
- Add an intrusion-detection check (+10 ms): latency **130 ms**; throughput ≈ 1,000 × 100/130 ≈ **769 req/s**.
- To restore 1,000 req/s one needs about 30% more servers (1,000/769 = 1.3), raising cost.

Resolution: use hardware acceleration (AES-NI), caching, CDN, TLS offload and risk-based selective encryption to balance both.

Conclusion: security cannot be dropped, so capacity and design are tuned to absorb its overhead.

Q3. Explain the major goal of NIST. Also explain the different layers in cloud computing. Discuss the NIST Cloud Reference Architecture and its key components. (2024, Feb 2024)

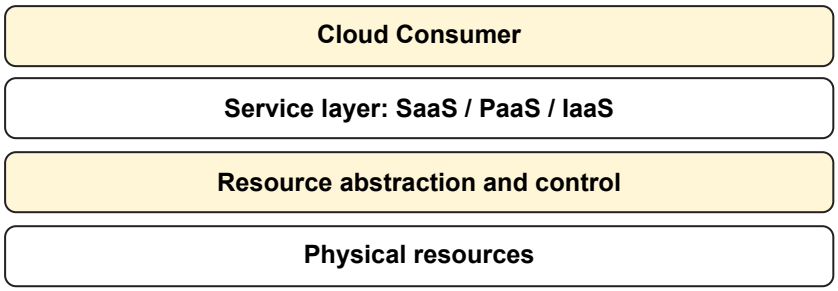
Goal of NIST: the National Institute of Standards and Technology aims to **define cloud computing, its models and a vendor-neutral reference architecture**, promoting standards, interoperability, portability and security so that government and industry can adopt the cloud confidently.

NIST definition: five characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), three service models (SaaS, PaaS, IaaS) and four deployment models (public, private, community, hybrid).

Layers in cloud computing:

1. **Physical resource layer:** servers, storage, network, facility.

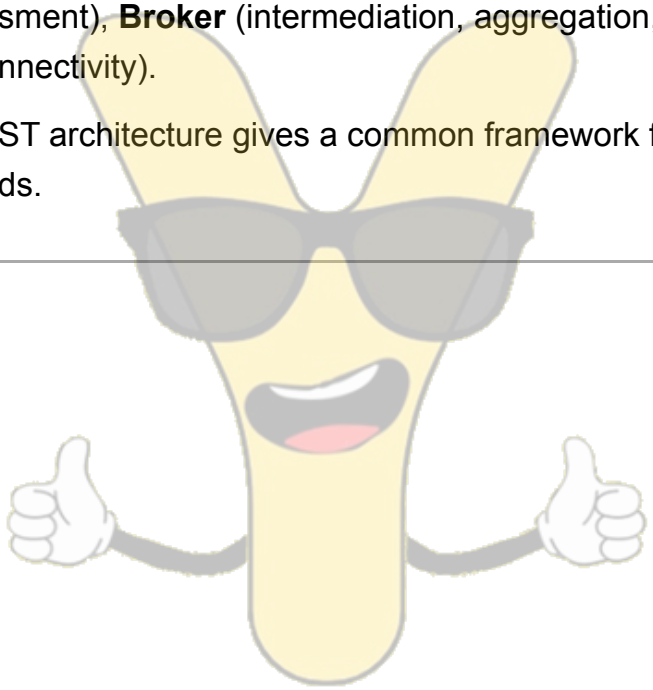
2. **Resource abstraction and control layer:** virtualization and management software.
3. **Service layer:** IaaS, PaaS, SaaS.



NIST layers

Key components (actors): Consumer (uses services), **Provider** (service orchestration, cloud service management, security and privacy), **Auditor** (independent assessment), **Broker** (intermediation, aggregation, arbitrage) and **Carrier** (network connectivity).

Conclusion: the NIST architecture gives a common framework for understanding and comparing clouds.



SECTION C Answers (≈500 Words Each)

Q1. Explain REST-based web services and their role in cloud applications. (Jan 2026)

REST (Representational State Transfer) is an architectural style for designing networked services. A **resource** (student, order) is identified by a **URI** and accessed through standard HTTP methods; the server returns a **representation** (JSON or XML).

HTTP method	Action	Example
GET	Read	GET /orders/5
POST	Create	POST /orders
PUT	Update	PUT /orders/5
DELETE	Remove	DELETE /orders/5

REST constraints: client-server, **stateless**, cacheable, uniform interface, layered system and optional code on demand.

```
GET /students/10 HTTP/1.1
Host: api.example.com
Accept: application/json
-> 200 OK  {"id":10,"name":"Asha"}
```

Role in cloud applications:

- Almost all cloud APIs (AWS S3, Google Cloud, Azure) are REST-based, so VMs, storage and services are controlled through HTTP.
- **Statelessness** lets servers scale horizontally behind load balancers.
- **Lightweight JSON** suits mobile and web clients.
- Caching reduces load and latency.
- Language and platform independence promotes interoperability and microservices.

REST vs SOAP: REST is simple and lightweight; SOAP is XML-based with strict contracts and built-in security standards.

Conclusion: REST is the standard way to access and compose cloud services.

Q2. Compare public, private and hybrid clouds. In what scenarios would an organization choose one? Conduct a cost analysis for a company moving to a hybrid model. (Jan 2025, Feb 2024)

Feature	Public	Private	Hybrid
Ownership	Provider, shared by many	Single organisation	Mix of both
Cost	Lowest, pay-per-use	Highest, own hardware	Moderate
Control and security	Lower	Highest	Selective
Scalability	Virtually unlimited	Limited by own capacity	Burst to public
Compliance	Harder	Easy	Sensitive data kept private
Example	AWS, Azure	Bank's own data centre, OpenStack	Private core + AWS burst

Choose:

- **Public:** start-ups, websites, testing, variable workloads, low sensitivity.
- **Private:** banks, defence, healthcare needing strict control and compliance.
- **Hybrid:** steady sensitive core with seasonal peaks (e-commerce, universities, cloud bursting, DR).

Cost analysis (monthly). A company has a steady load of 20 servers and bursts to 50 servers for 200 hours a month. Assumptions: private server amortised ₹5,000/month; public server ₹8/hour.

- **All private (sized for 50 servers):** 50 × 5,000 = **₹2,50,000**.
- **All public:** 20 × 720 h × 8 = ₹1,15,200 plus burst 30 × 200 h × 8 = ₹48,000 → **₹1,63,200**.
- **Hybrid:** private 20 × 5,000 = ₹1,00,000 plus public burst ₹48,000 → **₹1,48,000**.

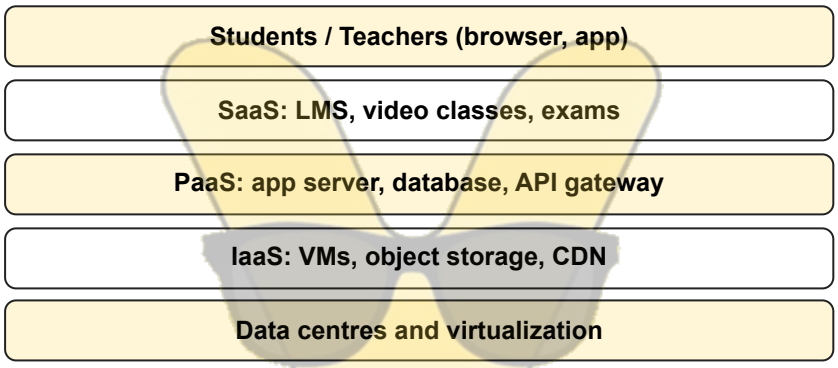
Hybrid is cheapest (saving ₹1,02,000 or 41% over all-private and ₹15,200 over all-public) while keeping sensitive data on private infrastructure. Additional costs: connectivity, integration and management tools.

Conclusion: hybrid balances cost, control and elasticity.

Q3. Describe layered cloud architecture design and analyze its implementation in an online education platform. (Jan 2025)

Layered cloud architecture organises the cloud into layers, each using services of the layer below.

1. **User/presentation layer:** web and mobile clients.
2. **SaaS/application layer:** end-user applications.
3. **PaaS/platform layer:** runtime, middleware, databases, APIs.
4. **IaaS/infrastructure layer:** VMs, storage, networks.
5. **Virtualization and physical layer:** hypervisors, servers, data centres.
   Cross-cutting: security, management, monitoring and billing.



Online education platform layers

Online education implementation:

- **Presentation:** learners access classes through browsers and mobile apps.
- **Application (SaaS):** course catalogue, live classes, quizzes and certificates as microservices.
- **Platform (PaaS):** managed database for results, message queues, authentication and API gateway.
- **Infrastructure (IaaS):** autoscaled VMs for peak exam traffic, object storage for recorded lectures and a CDN to stream video.
- **Management and security:** IAM, encryption of student data, monitoring and billing.

Analysis: layering gives **separation of concerns, independent scaling** (video layer scales without touching the grade database), easy replacement of components and clearer security zones. Challenges are added latency between layers and complex dependency management.

Conclusion: a layered design lets the platform handle sudden loads such as examinations economically.

Q4. Describe the components of a Cloud Provider and its responsibility for SaaS, PaaS and IaaS. (2024)

Components of a cloud provider (NIST):

- **Service deployment:** public/private/community/hybrid.
- **Service orchestration:** service layer (SaaS, PaaS, IaaS), resource abstraction and control layer, physical resource layer.
- **Cloud service management:** business support (customer management, billing, contracts), **provisioning and configuration** (rapid provisioning, resource changing, monitoring and reporting, metering, SLA management), **portability and interoperability**.
- **Security and privacy:** identity, data protection, compliance.

Responsibilities by model:

Layer	IaaS	PaaS	SaaS
Applications and data	Consumer	Consumer (app)	Provider
Runtime and middleware	Consumer	Provider	Provider
Operating system	Consumer	Provider	Provider
Virtualization, servers, storage, network	Provider	Provider	Provider
Physical facility and security	Provider	Provider	Provider

In IaaS the provider ensures infrastructure availability and virtualization; in PaaS it also manages the OS, middleware and platform scaling; in SaaS it manages the entire stack including application updates, and the consumer handles only user access and data input.

Q5. Explain Amazon S3 and its features. Describe the advantages of cloud storage. How does S3 support scalable and secure storage? (2024, Feb 2024)

Amazon S3 (Simple Storage Service) is an **object storage service** that stores any amount of data as **objects** (file + metadata, up to 5 TB each) in **buckets** (globally

unique names), accessed with a key through REST/HTTP APIs, the console or SDKs.

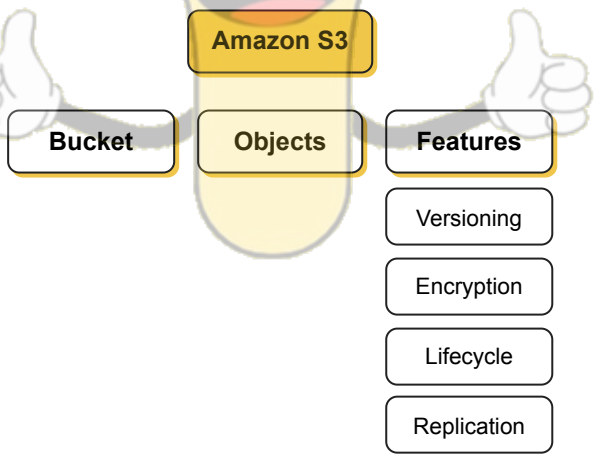
Features and functionality:

- **Durability and availability:** 99.999999999% (11 nines) durability by replicating across multiple Availability Zones.
- **Storage classes:** Standard, Intelligent-Tiering, Standard-IA, Glacier for archival, with lifecycle rules to move data automatically.
- **Versioning**, replication (cross-region) and event notifications.
- **Static website hosting** and integration with CloudFront CDN, Lambda and analytics.
- **Pay-as-you-go** pricing by storage, requests and transfer.

Scalability: virtually unlimited capacity, automatic scaling of request rate, no provisioning of disks.

Security: IAM policies and bucket policies, ACLs, **encryption at rest** (SSE-S3, SSE-KMS) and **in transit** (HTTPS), block public access, access logging, MFA delete and Object Lock.

Advantages of cloud storage: low cost, pay for use, elastic capacity, high durability, access anywhere, built-in backup and disaster recovery, no maintenance and easy sharing and integration.



S3 structure and features

Conclusion: S3 is the base of many cloud applications because it combines durability, scale and security.
