1. Definition

Cloud Computing is the delivery of computing services (like servers, storage, databases, networking, software, analytics, and intelligence) over the **internet ("the cloud")** to offer faster innovation, flexible resources, and economies of scale.

---

2. Key Characteristics

- **On-demand self-service** – Users can provision computing resources automatically.
- **Broad network access** – Services are available over the network and accessed through standard mechanisms.
- **Resource pooling** – Resources are pooled to serve multiple users using a multi-tenant model.
- **Rapid elasticity** – Resources can scale rapidly (up or down).
- **Measured service** – Usage is monitored, controlled, and billed (pay-as-you-go).

---

3. Service Models

1. **IaaS (Infrastructure as a Service)**
    - Provides virtualized computing resources over the internet.
    - *Examples*: AWS EC2, Google Compute Engine
    - **Users manage**: OS, apps, data
2. **PaaS (Platform as a Service)**
    - Provides a platform allowing customers to develop, run, and manage applications.
    - *Examples*: Google App Engine, Heroku
    - **Users manage**: Apps and data
3. **SaaS (Software as a Service)**
    - Delivers software over the internet, on a subscription basis.
    - *Examples*: Google Workspace, Microsoft 365
    - **Users manage**: Just their data

---

4. Deployment Models

1. **Public Cloud**
    - Services offered over the public internet, shared among multiple users.
    - *Providers*: AWS, Azure, Google Cloud
2. **Private Cloud**
    - Exclusive to a single organization. More control and security.
    - *Example*: VMware vSphere-based private data centers
3. **Hybrid Cloud**
    - Combination of public and private clouds with data/apps shared between them.
    - *Use Case*: Regulatory compliance + scalability
4. **Community Cloud**
    - Shared by several organizations with a common goal or requirement.

---

5. Benefits

- Cost-effective (no capital expense on hardware)
- Scalable and flexible
- High availability and reliability
- Disaster recovery
- Global reach
- Automatic updates and maintenance

---

6. Challenges

- Security and privacy concerns
- Downtime and internet dependency
- Limited control over infrastructure
- Compliance issues
- Vendor lock-in

---

7. Examples of Cloud Providers

- **Amazon Web Services (AWS)**
- **Microsoft Azure**
- **Google Cloud Platform (GCP)**
- **IBM Cloud**
- **Oracle Cloud**

---

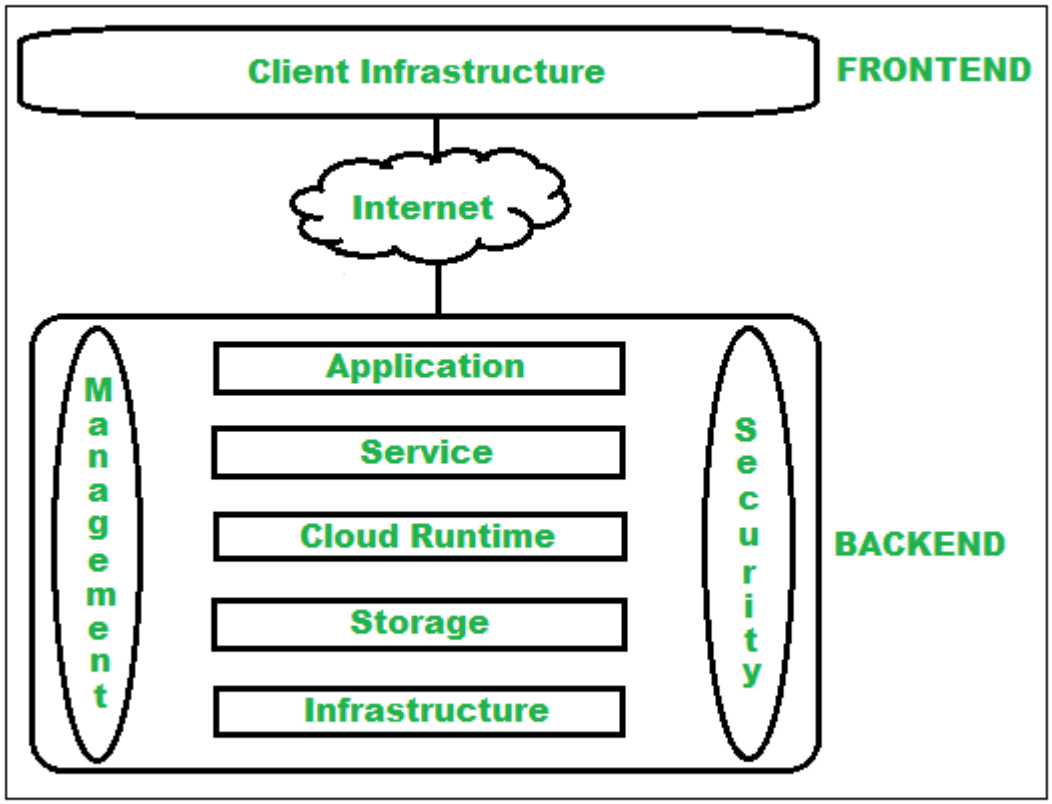
8. Popular Use Cases

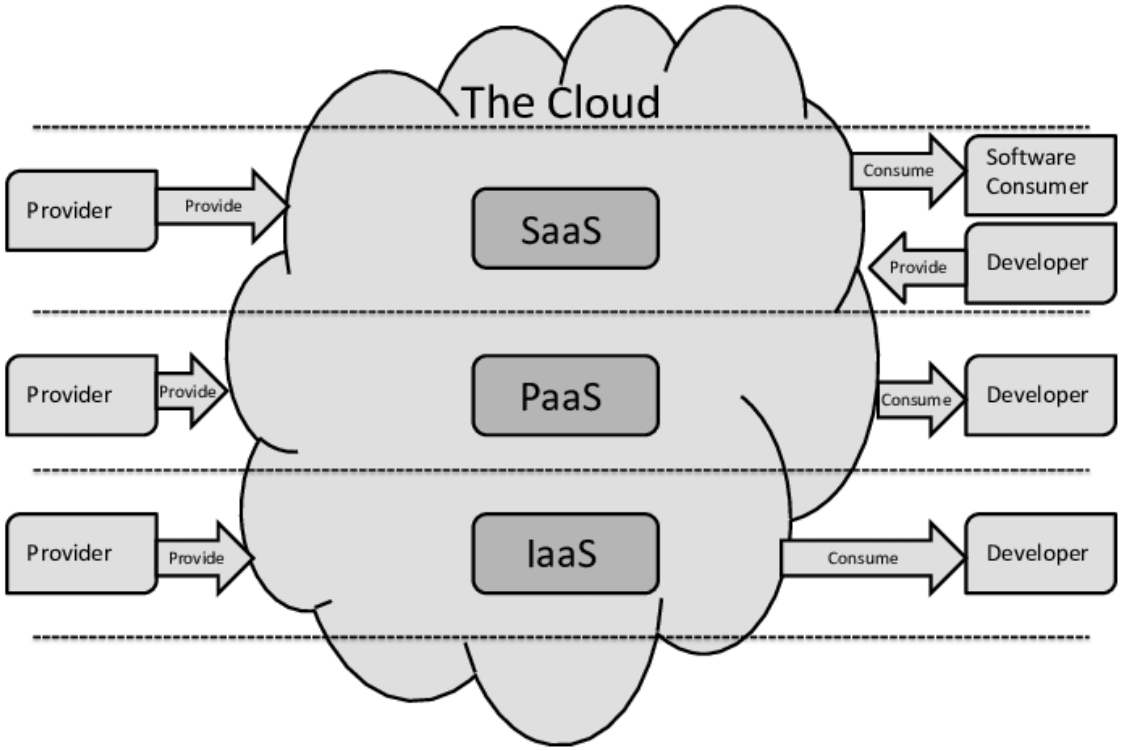
- Data backup and disaster recovery
- Hosting websites and blogs
- Big data analytics
- DevOps and CI/CD pipelines
- IoT and real-time data processing
- AI/ML model training and deployment

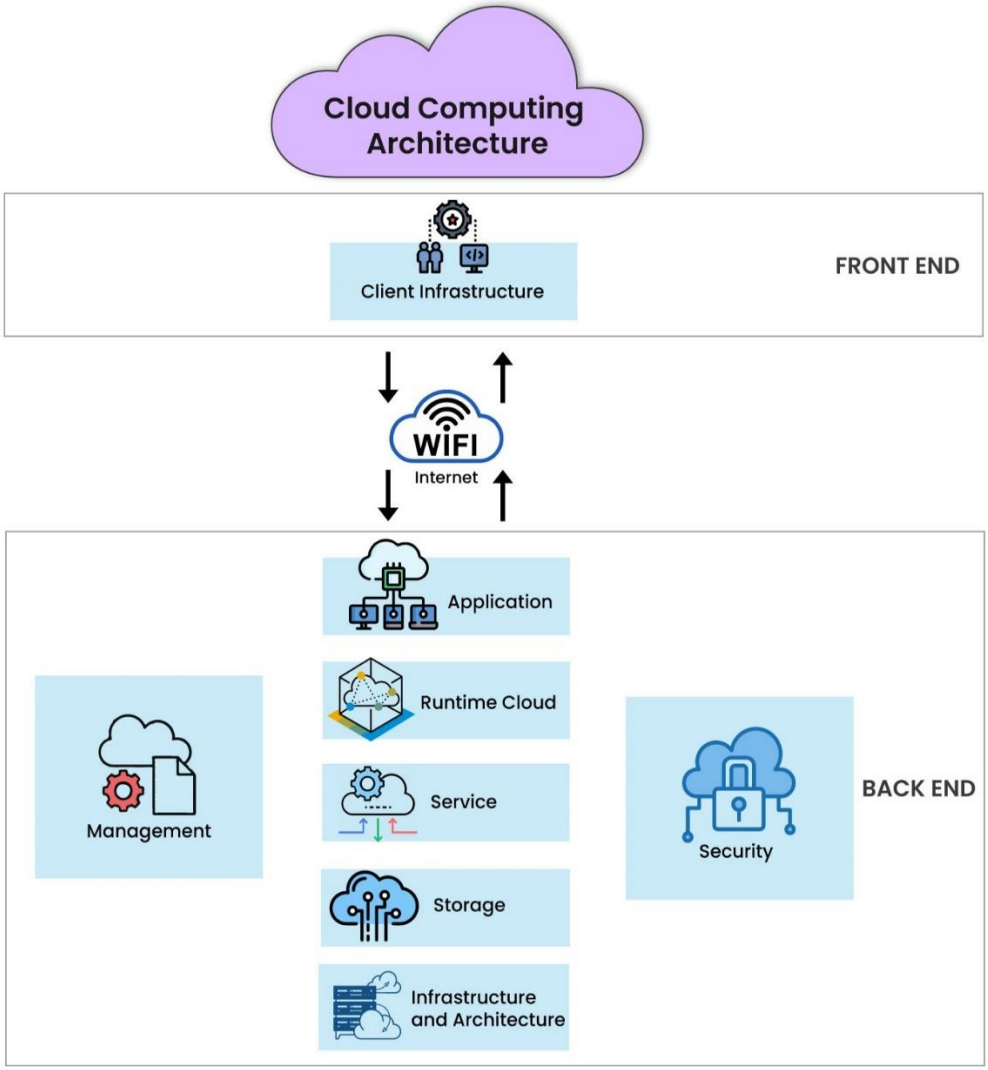
---

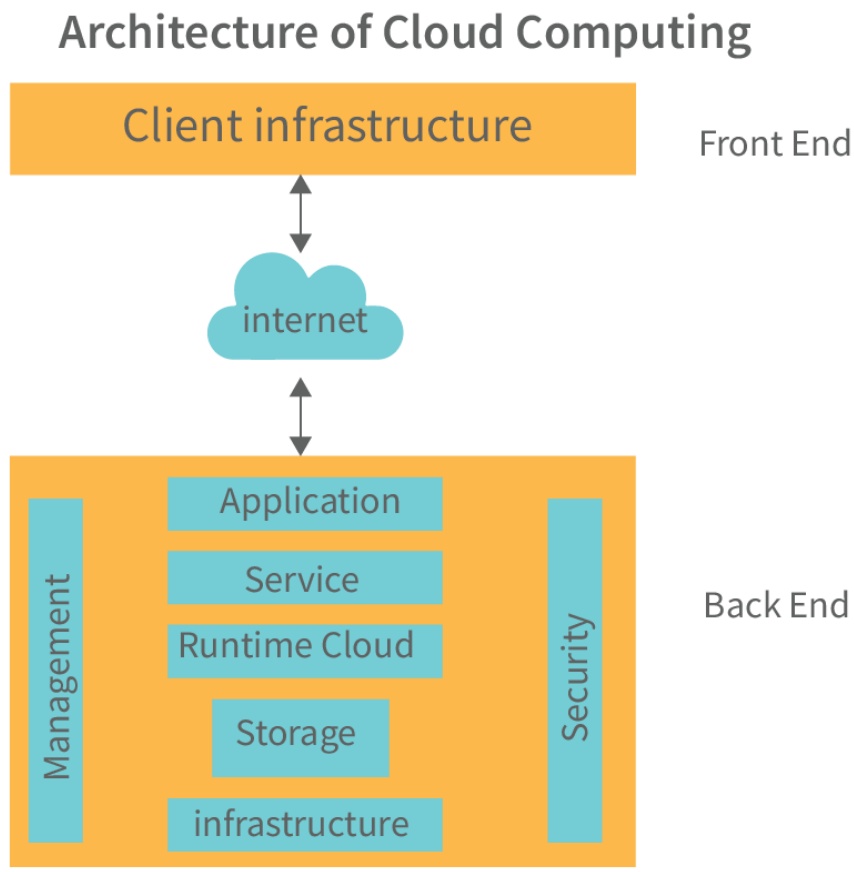
9. Cloud Security

- **Encryption** (data at rest and in transit)
- **Identity and Access Management (IAM)**
- **Firewalls & VPNs**
- **Regular audits and compliance checks**


Client Infrastructure
FRONTEND
Internet
Application
Service
Cloud Runtime
Storage
Infrastructure
Management
Security
BACKEND


The Cloud
Provider
Provide
SaaS
Consume
Software Consumer
Provide
Developer
Provider
Provide
PaaS
Consume
Developer
Provider
Provide
IaaS
Consume
Developer


Cloud Computing Architecture
Client Infrastructure
FRONT END
WiFI
Internet
Application
Runtime Cloud
Service
Storage
Infrastructure and Architecture
Management
Security
BACK END



InterviewBit

Definition & Key Concepts

- **Cloud Computing** = delivery of computing services (servers, storage, databases, networking, software, analytics, etc.) over the internet ("the cloud") on a pay-as-you-go basis.
- **Virtualization** is a core enabling technology — abstracts physical hardware to offer virtual resources.
- Underlying architectures often combine **Service-Oriented Architecture (SOA)** and **Event-Driven Architecture (EDA)**.

---

2. Characteristics

Characteristic	Description
On-demand self-service	Users can provision resources without human interaction.
Broad network access	Services accessible via standard network (e.g. via web, smartphone).
Resource pooling	Multiple users share physical resources (multi-tenancy).
Rapid elasticity	Resources can scale up or down quickly.
Measured service	Usage is monitored, reported, and billed.

---

3. Service Models

- **IaaS (Infrastructure as a Service)**
  Provides virtual machines, storage, networks. Users manage OS, middleware, apps.
  E.g. AWS EC2, Google Compute Engine
- **PaaS (Platform as a Service)**
  Provides platforms (runtime, dev tools, DB) so developers can build apps without managing underlying infra.
  E.g. Google App Engine, Heroku
- **SaaS (Software as a Service)**
  Delivers ready-to-use applications over the internet, managed by vendor.
  E.g. Gmail, Salesforce, Microsoft 365

---

4. Deployment Models

- **Public Cloud**: Third-party provider hosts services over the public internet (shared among multiple tenants).
- **Private Cloud**: Infrastructure dedicated to a single organization (on-premises or hosted).
- **Hybrid Cloud**: Combination of public + private, with data and application portability between them.
- **Community Cloud**: Shared by several organizations with common concerns (security, compliance).

---

5. Architecture: Frontend & Backend

- **Front End**: What the user sees — browser, client device, user interface.
- **Back End**: Service provider side — includes storage, servers, virtualization, management, security, networking, databases.

Components in Backend Architecture

1. **Client Infrastructure** (part of front end)
2. **Application / Service Layer**
3. **Runtime (execution environment / VMs / containers)**
4. **Storage**
5. **Infrastructure (servers, network, virtualization)**
6. **Management** (monitoring, scaling, orchestration)
7. **Security** (authentication, encryption, firewalls)
8. **Networking / Internet** (connects front end and back end)

---

6. Benefits & Challenges

Benefits

- Cost savings (reduced capital expenditure)
- Elasticity & scalability
- High availability & reliability
- Global accessibility
- Faster deployment & updates
- Disaster recovery & backup

Challenges

- Data security & privacy
- Downtime / outages
- Vendor lock-in
- Compliance / regulation constraints
- Limited control over infrastructure
- Performance / latency issues

---

7. Best Practices & Design Patterns

- Use **auto-scaling** to adapt to load
- Apply **circuit breaker patterns** when calling external services
- Use **bulkheads** to isolate failures in parts of system
- **Caching** to reduce latency
- **Retry / back-off** strategies for transient failures
- **Sharding / partitioning** for large databases
- **Security by design**: encryption, IAM, least privilege

Quiz / Practice Questions

1. What are the three main service models of cloud computing?
2. Explain the difference between IaaS and PaaS.
3. Name and describe two benefits and two challenges of cloud computing.
4. In the architecture, what is the role of the "management" component?
5. What is **vendor lock-in** in the cloud context, and how can you mitigate it?
6. Describe what a **hybrid cloud** is, with an example use case.
7. Which design pattern would help isolate a failure in one component so the rest of the system continues working?
8. Why is **measured service** important in cloud computing?

SLA in Cloud Computing – Notes

What is SLA?

SLA (Service Level Agreement) is a formal contract between a **cloud service provider (CSP)** and a **customer** that defines the **expected level of service**, **performance metrics**, and **responsibilities** of both parties.

Key Components of an SLA

1. **Service Description**
    - Specifies what services are being provided (e.g., IaaS, PaaS, SaaS).
    - Includes scope, functionality, and features.
2. **Performance Metrics**
    - Defines measurable parameters such as:
        - **Uptime/Downtime (Availability)** – e.g., 99.9% uptime
        - **Response Time** – Time taken to respond to a request
        - **Throughput** – Volume of data handled
        - **Latency** – Delay in processing
        - **Capacity and Scalability**
3. **Availability Guarantee**
    - Defines the **percentage of uptime** over a period (e.g., monthly or yearly).
    - Common cloud SLAs:
        - 99.9% uptime → ~8.76 hours of downtime/year
        - 99.99% → ~52.56 minutes/year
        - 99.999% → ~5.26 minutes/year
4. **Support and Maintenance**
    - Support hours (e.g., 24/7, business hours)
    - Incident response time
    - Escalation procedures
5. **Security and Compliance**
    - Details about data protection, privacy, and compliance with regulations (e.g., GDPR, HIPAA).
6. **Penalties and Remedies**
    - Compensation or service credits if SLA is violated.
    - Example: If uptime drops below 99.9%, user may receive 10% service credit.
7. **Monitoring and Reporting**
    - Tools used for performance tracking
    - Frequency of reporting (daily, weekly, monthly)
8. **Disaster Recovery and Backup**
    - RTO (Recovery Time Objective)
    - RPO (Recovery Point Objective)
9. **Change Management**
    - How service changes (upgrades, patches) are communicated and managed.
10. **Termination Conditions**

- Terms under which either party can terminate the agreement.

Types of SLAs

Type	Description
Customer-based	Tailored for a specific customer and includes all services they use
Service-based	Covers one service for all customers (e.g., Gmail availability)
Multilevel SLA	Combines multiple layers: corporate, customer, and service level

---

Importance of SLA in Cloud Computing

- Ensures **transparency** and **trust** between provider and user
- Provides a **benchmark** for evaluating service performance
- Helps in **resolving disputes** in case of service failures
- Sets **expectations** and encourages **accountability**

Common SLA Challenges

- **Ambiguous definitions** of metrics
- **Lack of monitoring tools**
- **Unrealistic expectations**
- **Rapidly changing cloud environments**

Best Practices for SLAs

- Use **clear and measurable** terms
- Review SLAs **regularly**
- Align SLA with **business goals**
- Include **escalation paths** and **contact points**
- Ensure **third-party** services are covered

Examples

- **AWS SLA:** Offers 99.99% for EC2, 99.9% for S3
- **Azure SLA:** 99.9% for virtual machines, 99.95% for storage
- **Google Cloud SLA:** 99.5% - 99.99% depending on service

Virtualization

Virtualization is a way to use one computer as if it were many. Before virtualization, most computers were only doing one job at a time, and a lot of their power was wasted. Virtualization lets you run several virtual computers on one real computer, so you can use its full power and do more tasks at once.

In cloud computing, this idea is taken further. Cloud providers use virtualization to split one big server into many smaller virtual ones, so businesses can use just what they need, no extra hardware, no extra cost.

Let us understand virtualization by taking a real-world example:

Suppose there is a company that requires servers for four different purposes:

- Store customer data securely
- Host an online shopping website
- Process employee payroll systems
- Run Social media campaign software for marketing

All these tasks require different things:

- The customer data server requires a lot of space and a Windows operating system.
- The online shopping website requires a high-traffic server and needs a Linux operating system.
- The payroll system requires greater internal memory (RAM) and must use a certain version of the operating system.

In order to fulfill these requirements, the company initially configures **four individual physical servers**, each for a different purpose. This implies that the company needs to purchase four servers, keep them running, and upgrade them individually, which is very expensive.

Now, by utilizing **virtualization**, the company can run these four applications on a few physical servers through multiple virtual machines (VMs). Each VM will behave as an independent server, possessing its own operating system and resources. Through this means, the company can cut down on expenses, conserve resources, and manage everything from a single location with ease.

Working of Virtualization

Virtualizations uses special software known as hypervisor, to create many virtual computers (cloud instances) on one physical computer. The Virtual Machines behave like actual computers but use the same physical machine.

Virtual Machines (Cloud Instances)

- After installing virtualization software, you can create one or more virtual machines on your computer.
- Virtual machines (VMs) behave like regular applications on your system.
- The real physical computer is called the **Host**, while the virtual machines are called **Guests**.
- A single host can run multiple guest virtual machines.
- Each guest can have its own operating system, which may be the same or different from the host OS.
- Every virtual machine functions like a standalone computer, with its own settings, programs, and configuration.
- VMs access system resources such as **CPU, RAM, and storage**, but they work as if they are using their own hardware.

Hypervisors

A hypervisor is the software that gets virtualization to work. It serves as an intermediary between the physical computer and the virtual machines. The hypervisor controls the virtual machines' use of the physical resources (such as the CPU and memory) of the host computer. For instance, if one virtual machine wants additional computing capability, it requests it from the hypervisor. The hypervisor ensures the request is forwarded to the physical hardware, and it's accomplished.

There exist two categories of hypervisors:

Type 1 Hypervisor (Bare-Metal Hypervisor):

- The hypervisor is installed directly onto the computer hardware, without an operating system sitting in between.
- It is highly efficient as it has a direct access to the resources of the computer.

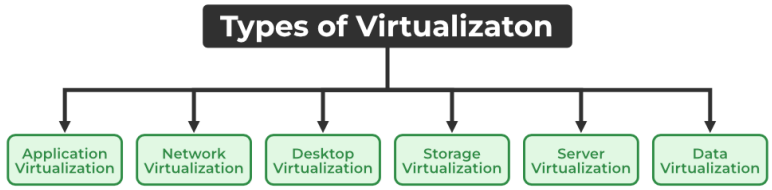
Type 2 Hypervisor:

- It is run over an installed operating system (such as Windows or macOS).
- It's employed when you need to execute more than one operating system on one machine.

Types of Virtualization

1. Application Virtualization

2. Network Virtualization
3. Desktop Virtualization
4. Storage Virtualization
5. Server Virtualization
6. Data virtualization



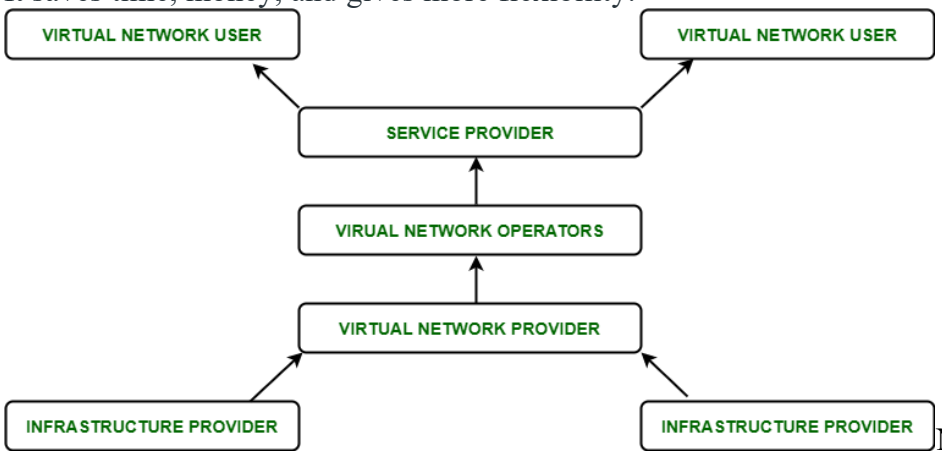
Types of Virtualization

1. Application Virtualization: Application virtualization enables remote access by which users can directly interact with deployed applications without installing them on their local machine. Your personal data and the applications settings are stored on the server, but you can still run it locally via the internet. It's useful if you need to work with multiple versions of the same software. Common examples include hosted or packaged apps.

Example: Microsoft Azure lets people use their applications without putting them on their own computers. Once this application is setup in the cloud then employees can use it from any device, like a laptop or tablet. It feels like the application is on their computer, but it's really running on Azure's servers. This makes things easier, faster, and safer for the company.

2. Network Virtualization: This allows multiple virtual networks to run on the same physical network, each operating independently. You can quickly set up virtual switches, routers, firewalls, and VPNs, making network management more flexible and efficient.

Example: Google Cloud is an example of Network Virtualization. Companies create their own networks using software instead of physical devices with the help of Google Cloud. They can set up things like IP addresses, firewalls, and private connections all in the cloud. This makes it easy to manage, change, and grow their network without buying any hardware. It saves time, money, and gives more flexibility.



Network

Virtualization

3. Desktop Virtualization: Desktop virtualization is a process in which you can create different virtual desktops that users can use from any device like laptop, tablet. It's great for users who need flexibility, as it simplifies software updates and provides portability.

Example: GeeksforGeeks is a Edtech company which uses services like **Amazon WorkSpaces** or **Google Cloud (GCP) Virtual Desktops** to give its team members access to the same coding setup with all the tools they required for the easy access of this team work.

Now their team members can easily log in from any device like a laptop, tablet, or even a phone and use a virtual desktop that will run perfectly in the cloud. This makes it easy for GeeksforGeeks company to manage, update, and keep everything secure without requirement of physical computers for everyone.

4. Storage Virtualization: This combines storage from different servers into a single system, making it easier to manage. It ensures smooth performance and efficient operations even when the underlying hardware changes or fails.

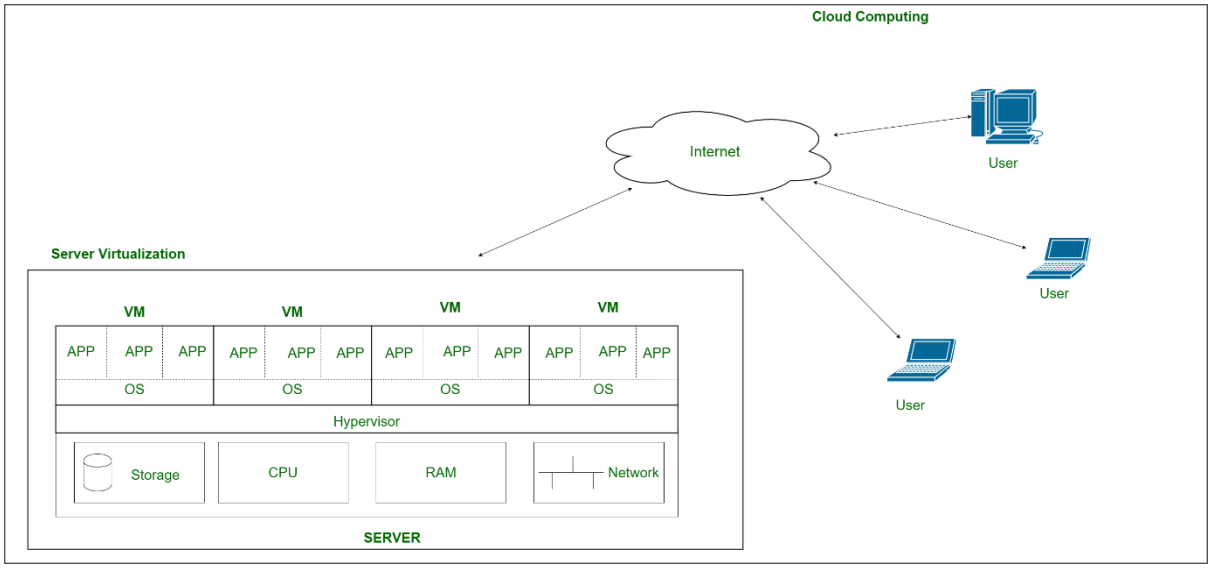
Example: Amazon S3 is an example of storage virtualization because in S3 we can easily store any amount of data from anywhere. Suppose a MNC have lots of files and data of company to store. By Amazon S3 company can store all their files and data in one place and access these from anywhere without any kind of issue in secure way.

5. Server Virtualization: This splits a physical server into multiple virtual servers, each functioning independently. It helps improve performance, cut costs and makes tasks like server migration and energy management easier.

Example: A startup company has a powerful physical server. This company can use server virtualization software like VMware vSphere, Microsoft Hyper-V or KVM to create more virtual machines(VMs) on that one server.

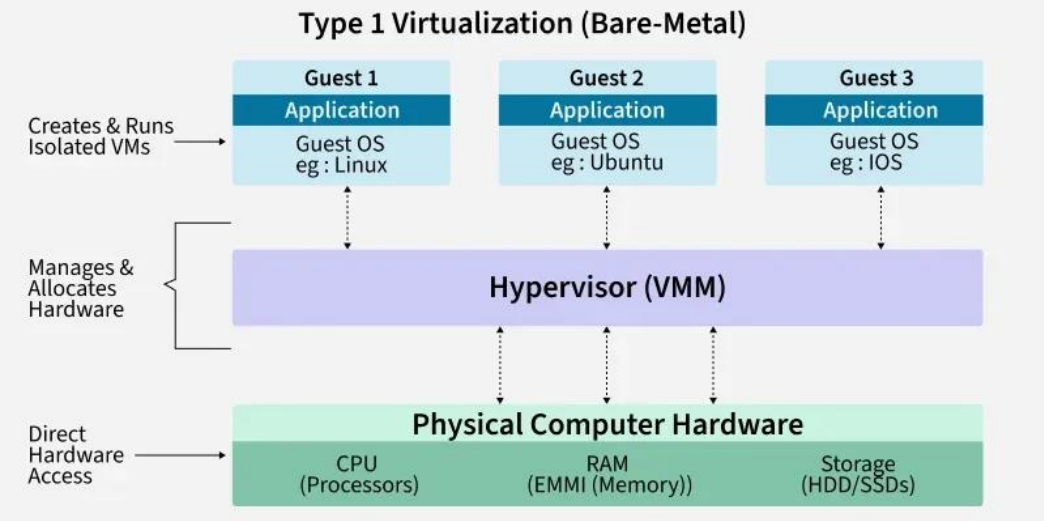
Each VM here is an isolated server, that runs on their own operating system(like Windows and Linux) and run it's own applications. For example, a company might run A web server on one VM, A database server on another VM, A file server on a third VM all on the same physical machine. This reduces costs, makes it easier to manage and back up servers, and allows quick recovery if one VM fails.

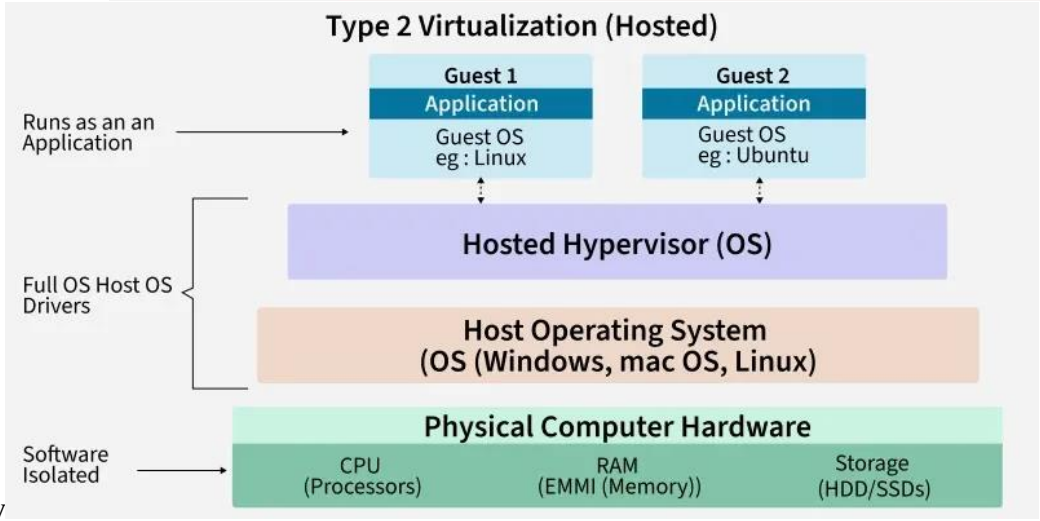
Server Virtualization



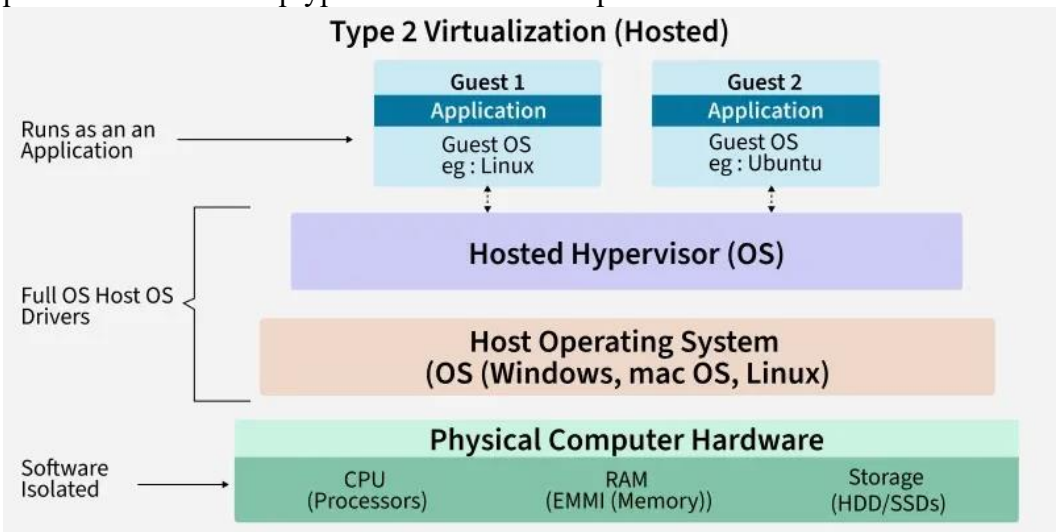
6. Data Virtualization: This brings data from different sources together in one place without needing to know where or how it's stored. It creates a unified view of the data, which can be accessed remotely via cloud services.

Example: Companies like Oracle and IBM offer solutions for this.





ty
pe1virtualisation.webptype1virtualisation.webp



Cloud storage is an online service where a third-party provider stores digital data on their remote servers, allowing users to access it via the internet from any device. It offers a scalable and cost-effective alternative to local storage, removing the need for organizations and individuals to purchase and maintain their own physical infrastructure. Key benefits include

data accessibility from anywhere, scalability to match data needs, and centralized data management with enhanced security features.

How It Works

1. **Offsite Data Storage:**

   Instead of storing files on local hard drives or company-owned servers, data is uploaded to servers located in data centers.

2. **Third-Party Management:**

   A cloud storage provider (like Google Cloud, Amazon S3, Dropbox, or Microsoft OneDrive) owns, manages, and maintains these servers and the associated infrastructure.

3. **Internet Access:**
   Users access their stored data and files through a public internet connection or a private network.

Key Benefits

- **Accessibility:**

  Data can be accessed from any device with an internet connection, facilitating remote work and collaboration.

- **Scalability:**

  Storage capacity can be easily expanded or reduced as needed, providing elastic capacity and cost efficiency.

- **Cost Savings:**

  It shifts storage expenses from capital investment in hardware to operational costs, eliminating the need for expensive data center maintenance.

- **Data Security & Durability:**

  Providers offer advanced security features, such as encryption, access controls, and backups, to protect data against loss or unauthorized access.

- **Disaster Recovery:**
  Storing data in a secure, off-site location provides a critical component of disaster recovery plans, ensuring data availability even if local systems fail.

Examples of Cloud Storage Providers

- **For Individuals:**

  Google Drive, iCloud, Dropbox, and pCloud offer services for personal file storage, backup, and sharing.

- **For Businesses:**

Providers like Google Cloud Storage, Amazon S3, and Microsoft Azure offer infrastructure-as-a-service (IaaS) solutions with advanced scalability and security for enterprise use.

Security In Cloud Computing :

Cloud computing which is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks. Community Cloud : These allow to a limited set of organizations or employees to access a shared cloud computing service environment.

Planning of security in Cloud Computing :

As security is a major concern in cloud implementation, so an organization have to plan for security based on some factors like below represents the three main factors on which planning of cloud security depends.

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.
- The risk in the deployment of the cloud depends on the types of cloud and service models.

Types of Cloud Security Controls :

There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of cloud security :

For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose it is essential to pick a cloud provider who offers the best security and is customized with the organization's infrastructure. Cloud security has a lot of benefits -

- **Centralized security :** Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
- **Reduced costs :** Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration
- **Reduced Administration :** It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
- **Reliability :** These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

When we are thinking about cloud security it includes various types of security like access control for authorized access, network segmentation for maintaining isolated data, encryption for encoded data transfer, vulnerability check for patching vulnerable areas, security monitoring for keeping eye on various security attacks and disaster recovery for backup and recovery during data loss.
There are different types of security techniques which are implemented to make the cloud computing system more secure such as SSL (Secure Socket Layer) Encryption, Multi Tenancy based Access Control, Intrusion Detection System, firewalls, penetration testing, tokenization, VPN (Virtual Private Networks), and avoiding public internet connections and many more techniques.
But the thing is not so simple how we think, even implementation of number of security techniques there is always security issues are involved for the cloud system. As cloud system is managed and accessed over internet so a lot of challenges arises during maintaining a secure cloud. Some cloud security challenges are

- Control over cloud data
- Misconfiguration
- Ever changing workload
- Access Management
- Disaster recovery

Conclusion
Cloud security is non-negotiable for any organization relying on cloud services. Implementing access control, encryption, network security, intrusion detection, and proactive monitoring ensures a resilient cloud security framework. Addressing cloud security challenges, continuously assessing threats, and enforcing best security practices will help organizations safeguard critical cloud infrastructure from cyber threats.

Cloud security is a responsibility that is shared between the cloud provider and the customer. There are basically three categories of responsibilities in the Shared Responsibility Model: responsibilities that are *always* the provider's, responsibilities that are *always* the customer's, and responsibilities that *vary depending on the service model*: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), such as cloud email.

The security responsibilities that are *always* the provider's are related to the safeguarding of the infrastructure itself, as well as access to, patching, and configuration of the physical hosts and the physical network on which the compute instances run and the storage and other resources reside.

The security responsibilities that are *always* the customer's include managing users and their access privileges (identity and access management), the safeguarding of cloud accounts from unauthorized access, the encryption and protection of cloud-based data assets, and managing its security posture (compliance).

The Top 7 Advanced Cloud Security Challenges

Because the public cloud does not have clear perimeters, it presents a fundamentally different security reality. This becomes even more challenging when adopting modern cloud approaches such as automated Continuous Integration and Continuous Deployment (CI/CD) methods, distributed serverless architectures, and ephemeral assets like Functions as a Service and containers.

Some of the advanced cloud-native security challenges and the multiple layers of risk faced by today's cloud-oriented organizations include:

1. **Increased Attack Surface**

   The public cloud environment has become a large and highly attractive attack surface for hackers who exploit poorly secured cloud ingress ports in order to access and disrupt workloads and data in the cloud. Malware, Zero-Day, Account Takeover and many other malicious threats have become a day-to-day reality.

2. **Lack of Visibility and Tracking**

   In the IaaS model, the cloud providers have full control over the infrastructure layer and do not expose it to their customers. The lack of visibility and control is further extended in the PaaS and SaaS cloud models. Cloud customers often cannot effectively identify and quantify their cloud assets or visualize their cloud environmets.

3. **Ever-Changing Workloads**

   Cloud assets are provisioned and decommissioned dynamically—at scale and at velocity. Traditional security tools are simply incapable of enforcing protection policies in such a flexible and dynamic environment with its ever-changing and ephemeral workloads.

4. **DevOps, DevSecOps and Automation**

   Organizations that have embraced the highly automated DevOps CI/CD culture must ensure that appropriate security controls are identified and embedded in code and templates early in the development cycle. Security-related changes implemented *after* a workload has been deployed in production can undermine the organization's security posture as well as lengthen time to market.

5. **Granular Privilege and Key Management**

Often cloud user roles are configured very loosely, granting extensive privileges beyond what is intended or required. One common example is giving database delete or write permissions to untrained users or users who have no business need to delete or add database assets. At the application level, improperly configured keys and privileges expose sessions to security risks.

6. **Complex Environments**

   Managing security in a consistent way in the hybrid and multicloud environments favored by enterprises these days requires methods and tools that work seamlessly across public cloud providers, private cloud providers, and on-premise deployments—including branch office edge protection for geographically distributed organizations.

7. **Cloud Compliance and Governance**

   All the leading cloud providers have aligned themselves with most of the well-known accreditation programs such as PCI 3.2, NIST 800-53, HIPAA and GDPR. However, customers are responsible for ensuring that their workload and data processes are compliant. Given the poor visibility as well as the dynamics of the cloud environment, the compliance audit process becomes close to mission impossible unless tools are used to achieve continuous compliance checks and issue real-time alerts about misconfigurations.

The 6 Pillars of Robust Cloud Security

While cloud providers such as Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) offer many cloud native security features and services, supplementary third-party solutions are essential to achieve enterprise-grade cloud workload protection from breaches, data leaks, and targeted attacks in the cloud environment. Only an integrated cloud-native/third-party security stack provides the centralized visibility and policy-based granular control necessary to deliver the following industry best practices:

1. **Granular, policy-based IAM and authentication controls across complex infrastructures**

   Work with groups and roles rather than at the individual IAM level to make it easier to update IAM definitions as business requirements change. Grant only the minimal access privileges to assets and APIs that are essential for a group or role to carry out its

tasks. The more extensive privileges, the higher the levels of authentication. And don't neglect good IAM hygiene, enforcing strong password policies, permission time-outs, and so on.

2. **Zero-trust cloud network security controls across logically isolated networks and micro-segments**

   Deploy business-critical resources and apps in logically isolated sections of the provider's cloud network, such as Virtual Private Clouds (AWS and Google) or vNET (Azure). Use subnets to micro-segment workloads from each other, with granular security policies at subnet gateways. Use dedicated WAN links in hybrid architectures, and use static user-defined routing configurations to customize access to virtual devices, virtual networks and their gateways, and public IP addresses.

3. **Enforcement of virtual server protection policies and processes such as change management and software updates**:

   Cloud security vendors provide robust Cloud Security Posture Management, consistently applying governance and compliance rules and templates when provisioning virtual servers, auditing for configuration deviations, and remediating automatically where possible.

4. **Safeguarding all applications (and especially cloud-native distributed apps) with a next-generation web application firewall**

   This will granularly inspect and control traffic to and from web application servers, automatically updates WAF rules in response to traffic behavior changes, and is deployed closer to microservices that are running workloads.

5. **Enhanced data protection**

   Enhanced data protection with encryption at all transport layers, secure file shares and communications, continuous compliance risk management, and maintaining good data storage resource hygiene such as detecting misconfigured buckets and terminating orphan resources.

6. **Threat intelligence that detects and remediates known and unknown threats in real-time**

   Third-party cloud security vendors add context to the large and diverse streams of cloud-native logs by intelligently cross-referencing aggregated log data with internal

data such as asset and configuration management systems, vulnerability scanners, etc. and external data such as public threat intelligence feeds, geolocation databases, etc. They also provide tools that help visualize and query the threat landscape and promote quicker incident response times. AI-based anomaly detection algorithms are applied to catch unknown threats, which then undergo forensics analysis to determine their risk profile. Real-time alerts on intrusions and policy violations shorten times to remediation, sometimes even triggering auto-remediation workflows.