1. Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

2. **Resources Pooling**
3. **On-Demand Self-Service**
4. **Easy Maintenance**
5. **Scalability And Rapid Elasticity**
6. **Economical**
7. **Measured And Reporting Service**
8. **Security**
9. **Automation**
10. **Resiliency And Availability**
11. **Large Network Access**
12. **Work From Any Location**
13. **Multi-Tenancy**
14. **Flexibility**
15. **Service Excellence**
16. **Comfortable Payment Structure**

1. RESOURCES POOLING

Resource pooling is one of the essential characteristics of Cloud Computing. Resource pooling means a cloud service provider can share resources among several clients, providing everyone with a different set of services per their requirements. It is a multi-client strategy that can be applied to data storage, processing, and bandwidth-provided services. The real-time administration process of allocating resources doesn't conflict with the client's experience.

2. ON-DEMAND SELF-SERVICE

It is one of the significant and essential features of Cloud Computing. It enables the client to constantly monitor the server uptime, abilities, and allotted network storage. This is a fundamental characteristic of Cloud Computing, and a client can likewise control the computing abilities as per his needs.

3. EASY MAINTENANCE

This is one of the best cloud characteristics. The servers are effortlessly maintained, and the downtime sometimes remains low or absolutely zero. Cloud Computing powered resources undergo several updates frequently to optimize their capabilities and potential. The updates are more viable with the devices and perform quicker than the previous versions.

4. SCALABILITY AND RAPID ELASTICITY

A key characteristic and benefit of cloud computing is its rapid scalability. This cloud characteristic enables the cost-effective running of workloads that require a vast number of servers but only for a short period. Many clients have such workloads, which can be run very cost-effectively because of the rapid scalability of Cloud Computing.

5. ECONOMICAL

This cloud characteristic helps in reducing the IT expenditure of the organizations. In Cloud Computing, the client needs to pay the administration for the space they have used. There is no covered-up or additional charge which needs to be paid. The administration is economical, and more often than not, some space is allotted for free.

6. MEASURED AND REPORTING SERVICE

Reporting services are one of the many cloud characteristics that make it the best choice for organizations. Measuring & reporting service is helpful for both cloud providers and their clients. It enables both the provider and the client to monitor and report what services have been used and for what purpose. This helps in monitoring billing and ensuring the optimum usage of resources.

7. SECURITY

Data security is one of the best characteristics of Cloud Computing. Cloud services create a copy of the data that is stored to prevent any form of data loss. If one server loses the data by any chance, the copy version is restored from the other server. This feature comes handy when several users work on a particular file in real-time, and a file suddenly gets corrupted.

8. AUTOMATION

Automation is an essential characteristic of cloud computing. The ability of cloud computing to automatically install, configure, and maintain a cloud service is known as automation in cloud computing. In simple terms, it is the process of making the most of technology and reducing manual effort. However, achieving automation in the cloud ecosystem is not so easy. It requires installing and deploying virtual machines, servers, and large storage. Upon successful deployment, these resources require constant maintenance as well.

9. RESILIENCE

Resilience in cloud computing means the ability of the service to quickly recover from any disruption. A cloud's resilience is measured by how fast its servers, databases, and network system restarts and recover from any harm or damage. Availability is another major characteristic of cloud computing. Since cloud services can be accessed remotely, there is no geographic restriction or limitation when it comes to utilizing cloud resources.

10. LARGE NETWORK ACCESS

A big part of the cloud characteristics is its ubiquity. The client can access the cloud data or transfer the data to the cloud from any place just with a device and internet connection. These capacities are accessible everywhere in the organization and get to with the help of the internet. Cloud providers save that large network access by monitoring and guaranteeing different measurements that reflect how clients access cloud resources and data: latency, access time, data throughput, etc.

11. WORK FROM ANY LOCATION

Remote working is one of the primary **features of cloud computing. It** enables users to work remotely or from any location on the planet. Users will be able to access corporate data via mobile devices such as laptops and smartphones. It also ensures that every user can connect quickly. Employees that work remotely or live in another location can communicate with one another and do their jobs.

12. MULTI-TENANCY

One of the best **characteristics of Cloud Computing** is its Multi-Tenancy. Multi-Tenancy is a software architecture that allows a single program instance to serve several user groups. It signifies that numerous cloud provider customers are sharing the same computing resources. Although they share the same computing resources, each Cloud customer's data is kept completely separate and safe.

13. FLEXIBILITY

The company must scale as the competition develops. Users that use the traditional hosting technique will have to switch service providers. Users benefit from greater freedom when they host their data in the cloud. Scaling does not require the server to be restarted and can be done anytime. There are a variety of payment alternatives also available for the users. This implies businesses won't have to spend too much on resources they don't need.

14. SERVICE EXCELLENCE

Cloud computing ensures that users receive the highest level of service possible. The benefits outlined in Service Level Agreements must include continuous availability and comprehensive resources, performance, and bandwidth. Any compromise on these services will result in a loss of clients and a decrease in popularity.

15. COMFORTABLE PAYMENT STRUCTURE

The payment structure is critical since it aids in the cost-cutting process. Because of the additional functionality, cloud computing choices come with a range of prices. Users find the payment option to be simple to use, and it allows them to save time when making payments regularly.

Advantages and Disadvantages of Cloud Computing
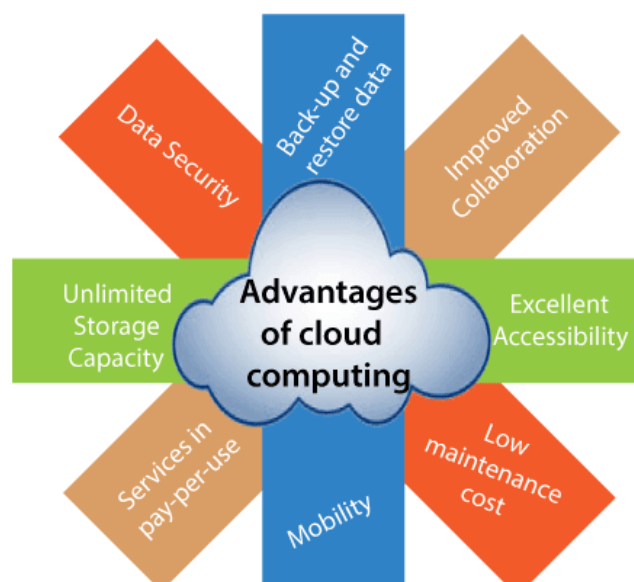
1) Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

2) Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3) Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

4) Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5) Mobility

Cloud computing allows us to easily access all cloud data via mobile.

6) IServices in the pay-per-use model

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

7) Unlimited storage capacity

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

8) Data security

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

Disadvantages of Cloud Computing

A list of the disadvantage of cloud computing is given below -

1) Internet Connectivity

As you know, in cloud computing, every data (image, audio, video, etc.) is stored on the cloud, and we access these data through the cloud by using the internet connection. If you do not have good internet connectivity, you cannot access these data. However, we have no any other way to access data from the cloud.

2) Vendor lock-in

Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving from one cloud to another.

3) Limited Control

As we know, cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.

4) Security

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.

2.
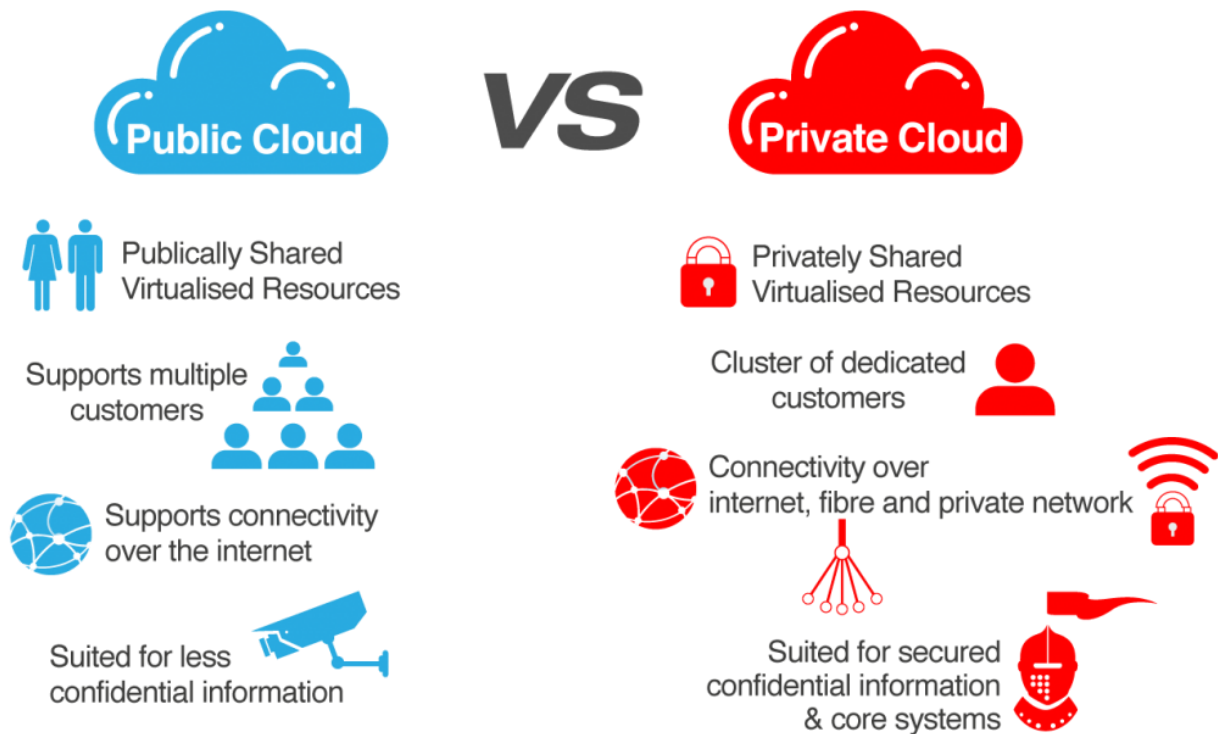
Models for Deployment in cloud computing

Deployment Models

The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's nature and purpose. The location of the servers you're utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types.

Different types of cloud computing deployment models are:

1. Public cloud

2. Private cloud
3. Hybrid cloud
4. Community cloud
5. Multi-cloud

Let us discuss them one by one:

1. Public Cloud

The public cloud makes it possible for anybody to access systems and services. The public cloud may be less secure as it is open for everyone. The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or major industry groups. The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer. It is a type of cloud hosting that allows customers and users to easily access systems and services. This form of cloud computing is an excellent example of cloud hosting, in which service providers supply services to a variety of customers. In this arrangement, storage backup and retrieval services are given for free, as a subscription, or on a per-use basis. Example: Google App Engine etc.

Advantages of the public cloud model:
- **Minimal Investment:** Because it is a pay-per-use service, there is no substantial upfront fee, making it excellent for enterprises that require immediate access to resources.
- **No setup cost:** The entire infrastructure is fully subsidized by the cloud service providers, thus there is no need to set up any hardware.
- **Infrastructure Management is not required:** Using the public cloud does not necessitate infrastructure management.
- **No maintenance:** The maintenance work is done by the service provider (Not users).
- **Dynamic Scalability:** To fulfill your company's needs, on-demand resources are accessible.

2. Private Cloud

The private cloud deployment model is the exact opposite of the public cloud deployment model. It's a one-on-one environment for a single user (customer). There is no need to share your hardware with anyone else. The distinction between private and public cloud is in how you handle all of the hardware. It is also called the "internal cloud" & it refers to the ability to access systems and services within a given border or organization. The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization's IT department.
The private cloud gives the greater flexibility of control over cloud resources.

Advantages of the private cloud model:

- **Better Control:** You are the sole owner of the property. You gain complete command over service integration, IT operations, policies, and user behavior.
- **Data Security and Privacy:** It's suitable for storing corporate information to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved.
- **Supports Legacy Systems:** This approach is designed to work with legacy systems that are unable to access the public cloud.
- **Customization:** Unlike a public cloud deployment, a private cloud allows a company to tailor its solution to meet its specific needs.

3. Hybrid cloud

By bridging the public and private worlds with a layer of proprietary software, hybrid cloud computing gives the best of both worlds. With a hybrid solution, you may host the app in a safe environment while taking advantage of the public cloud's cost savings. Organizations can move data and applications between different clouds using a combination of two or more cloud deployment methods, depending on their needs.

Advantages of the hybrid cloud model:
- **Flexibility and control:** Businesses with more flexibility can design personalized solutions that meet their particular needs.
- **Cost:** Because public clouds provide for scalability, you'll only be responsible for paying for the extra capacity if you require it.
- **Security:** Because data is properly separated, the chances of data theft by attackers are considerably reduced.

4. Community cloud

It allows systems and services to be accessible by a group of organizations. It is a distributed system that is created by integrating the services of different clouds to address the specific needs of a community, industry, or business. The infrastructure of the community could be shared between the organization which has shared concerns or tasks. It is generally managed by a third party or by the combination of one or more organizations in the community.

Advantages of the community cloud model:
- **Cost Effective:** It is cost-effective because the cloud is shared by multiple organizations or communities.
- **Security:** Community cloud provides better security.
- **Shared resources:** It allows you to share resources, infrastructure, etc. with multiple organizations.
- **Collaboration and data sharing:** It is suitable for both collaboration and data sharing.
-

5. Multi-cloud

We're talking about employing multiple cloud providers at the same time under this paradigm, as the name implies. It's similar to the hybrid cloud deployment approach, which combines public and private cloud resources. Instead of merging private and public clouds, multi-cloud uses many public clouds. Although public cloud providers provide numerous tools to improve the reliability of their services, mishaps still occur. It's quite rare that two distinct clouds would have an incident at the same moment. As a result, multi-cloud deployment improves the high availability of your services even more.

Advantages of a multi-cloud model:

- You can mix and match the best features of each cloud provider's services to suit the demands of your apps, workloads, and business by choosing different cloud providers.
- **Reduced Latency:** To reduce latency and improve user experience, you can choose cloud regions and zones that are close to your clients.
- **High availability of service:** It's quite rare that two distinct clouds would have an incident at the same moment. So, the multi-cloud deployment improves the high availability of your services.

1. IAAS: Infrastructure As A Service (IAAS) is means of delivering computing infrastructure as on-demand services. It is one of the three fundamental cloud service models. The user purchases servers, software data center space, or network equipment and rent those resources through a fully outsourced, on-demand service model. It allows dynamic scaling and the resources are distributed as a service. It generally includes multiple-user on a single piece of hardware.

2. PAAS: Platform As A Service (PAAS) is a cloud delivery model for applications composed of services managed by a third party. It provides elastic scaling of your application which allows developers to build applications and services over the internet and the deployment models include public, private and hybrid.

3. SAAS: Software As A Service (SAAS) allows users to run existing online applications and it is a model software that is deployed as a hosting service and is accessed over Output Rephrased/Re-written Text the internet or software delivery model during which software and its associated data are hosted centrally and accessed using their client, usually an online browser over the web. SAAS services are used for the development and deployment of modern applications.

Difference between IAAS, PAAS and SAAS :

Basis Of	IAAS	PAAS	SAAS
Stands for	Infrastructure as a service.	Platform as a service.	Software as a service.
Uses	IAAS is used by network architects.	PAAS is used by developers.	SAAS is used by the end user.
Access	IAAS gives access to the resources like virtual machines and virtual storage.	PAAS gives access to run time environment to deployment and development tools for application.	SAAS gives access to the end user.
Model	It is a service model that provides virtualized computing resources over the internet.	It is a cloud computing model that delivers tools that are used for the development of applications.	It is a service model in cloud computing that hosts software to make it available to clients.

Basis Of	IAAS	PAAS	SAAS
Technical understanding.	It requires technical knowledge.	Some knowledge is required for the basic setup.	There is no requirement about technicalities company handles everything.
Popularity.	It is popular among developers and researchers.	It is popular among developers who focus on the development of apps and scripts.	It is popular among consumers and companies, such as file sharing, email, and networking.
Cloud services.	Amazon Web Services, sun, vCloud Express.	Facebook, and Google search engine.	MS Office web, Facebook and Google Apps.
Enterprise services.	AWS virtual private cloud.	Microsoft Azure.	IBM cloud analysis.
Outsourced cloud services.	Salesforce	Force.com, Gigaspaces.	AWS, Terremark
User Controls	Operating System, Runtime, Middleware, and Application data	Data of the application	Nothing

Advantages of IaaS
- The resources can be deployed by the provider to a customer's environment at any given time.
- Its ability to offer the users to scale the business based on their requirements.
- The provider has various options when deploying resources including virtual machines, applications, storage, and networks.
- It has the potential to handle an immense number of users.
- It is easy to expand and saves a lot of money. Companies can afford the huge costs associated with the implementation of advanced technologies.

Advantages of PaaS –

- Programmers need not worry about what specific database or language the application has been programmed in.
- It offers developers the to build applications without the overhead of the underlying operating system or infrastructure.
- Provides the freedom to developers to focus on the application's design while the platform takes care of the language and the database.

Advantages of SaaS
- It is a cloud computing service category providing a wide range of hosted capabilities and services. These can be used to build and deploy web-based software applications.
- It provides a lower cost of ownership than on-premises software. The reason is it does not require the purchase or installation of hardware or licenses.
- It can be easily accessed through a browser along a thin client.

Microsoft Azure, formerly known as Windows Azure, is

Microsoft's public cloud computing platform. It provides a broad range of cloud services, including compute, analytics, storage and networking. Users can pick and choose from these services to develop and scale new applications or run existing applications in the public cloud.

Azure products and services

Microsoft sorts Azure cloud services into nearly two dozen categories. Each category can include numerous specific instance or service types. The most popular service categories include the following:

Compute. These services enable a user to deploy and manage VMs, containers and batch jobs, as well as support remote application access. Compute resources created within the Azure cloud can be configured with either public IP addresses or private IP addresses, depending on whether the resource needs to be accessible to the outside world.

Mobile. These products help developers build cloud applications for mobile devices, providing notification services, support for back-end tasks, tools for building application program interfaces (APIs) and the ability to couple geospatial context with data.

Web. These services support the development and deployment of web applications. They also offer features for search, content delivery, API management, notification and reporting.

Storage. This category of services provides scalable cloud storage for structured and unstructured data. It also supports big data projects, persistent storage and archival storage.

Analytics. These services provide distributed analytics and storage, as well as features for real-time analytics, big data analytics, data lakes, machine learning, business intelligence, internet of things (IoT) data streams and data warehousing.

Networking. This group includes virtual networks, dedicated connections and gateways, as well as services for traffic management and diagnostics, load balancing, DNS hosting and network protection against distributed denial-of-service (DDoS) attacks.

Media and content delivery network (CDN). These CDN services include on-demand streaming, digital rights protection, encoding, and media playback and indexing.

Integration. These are services for server backup, site recovery and connecting private and public clouds.

Identity. These offerings ensure only authorized users can access Azure services and help protect encryption keys and other sensitive information in the cloud. Services include support for Azure Active Directory and multifactor authentication.

IoT. These services help users capture, monitor and analyze IoT data from sensors and other devices. Services include notifications, analytics, monitoring and support for coding and execution.

DevOps. This group provides project and collaboration tools, such as Azure DevOps -- formerly Visual Studio Team Services -- that facilitate DevOps software development processes. It also offers features for application diagnostics, DevOps tool integrations and test labs for build tests and experimentation.

Development. These services help application developers share code, test applications and track potential issues. Azure supports a range of application programming languages, including JavaScript, Python, .NET and Node.js. Tools in this category also include support for Azure DevOps, software development kits (SDKs) and blockchain.

Security. These products provide capabilities to identify and respond to cloud security threats, as well as manage encryption keys and other sensitive assets.

AI and machine learning. This is a wide range of services that a developer can use to infuse AI, machine learning and cognitive computing capabilities into applications and data sets.

Containers. These services help an enterprise create, register, orchestrate and manage huge volumes of containers in the Azure cloud, using common container platforms such as Docker and orchestration platforms including Kubernetes.

Databases. This category includes database as a service (DBaaS) offerings for SQL and NoSQL, as well as other database instances -- such as Azure Cosmos DB and Azure Database for PostgreSQL. It also includes Azure SQL Data Warehouse support, caching, and hybrid database integration and migration features. Azure SQL is the platform's flagship database service. It is a relational database that provides SQL functionality without the need for deploying a SQL server.

Migration. This suite of tools helps an organization estimate workload Migration costs and perform the actual migration of workloads from local data centers to the Azure cloud.

Management and governance. These services provide a range of backup, recovery, compliance, automation, scheduling and monitoring tools that can help a cloud administrator manage an Azure deployment.

Mixed reality. These services are designed to help developers create content for the Windows Mixed Reality environment.

Blockchain. The Azure Blockchain Service lets you join a blockchain consortium or create your own.

Intune. [Microsoft Intune](#) can be used to enroll user devices, thereby making it possible to push security policies and mobile apps to those devices. Mobile apps can be deployed either to groups of users or to a collection of devices. Intune also provides tools for tracking which apps are being used. A remote wipe feature allows the organization's data to be securely removed from devices without removing a user's mobile apps in the process.

Azure for DR and backup

Some organizations use Azure for data backup and disaster recovery. Organizations can also use Azure as an alternative to their own data center storage. Public clouds have proven ideal for high-volume, short-duration tasks such as data analytics. Organizations can use almost limitless storage capacity in the cloud to store vast data sets, perform analytics tasks and then dismiss data as it ages or becomes unusable -- all without procuring or deploying hardware in a local data center. This type of *utility computing* has been a fundamental driver behind public cloud adoption since its inception.

Amazon EC2

Amazon Elastic Compute Cloud (**Amazon EC2**) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

Features of Amazon EC2

Amazon EC2 provides the following features:

- Virtual computing environments, known as instances
- Preconfigured templates for your instances, known as Amazon Machine Images (AMIs), that package the bits you need for your server (including the operating system and additional software)
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as instance types
- Secure login information for your instances using key pairs (AWS stores the public key, and you store the private key in a secure place)
- Storage volumes for temporary data that's deleted when you stop, hibernate, or terminate your instance, known as instance store volumes
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as Amazon EBS volumes

- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as Regions and Availability Zones
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
- Static IPv4 addresses for dynamic cloud computing, known as Elastic IP addresses
- Metadata, known as tags, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS Cloud, and that you can optionally connect to your own network, known as virtual private clouds (VPCs)

Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization, multiple operating systems and applications can run on same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

In other words, one of the main cost effective, hardware reducing, and energy saving techniques used by cloud providers is virtualization. Virtualization allows to share a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to a physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.
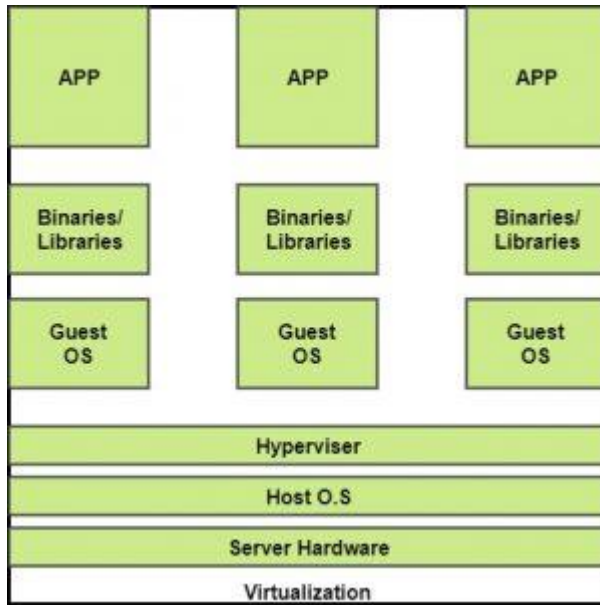
The machine on which the virtual machine is going to be built is known as Host Machine and that virtual machine is referred as a Guest Machine.

BENEFITS OF VIRTUALIZATION
1. More flexible and efficient allocation of resources.
2. Enhance development productivity.
3. It lowers the cost of IT infrastructure.
4. Remote access and rapid scalability.
5. High availability and disaster recovery.
6. Pay peruse of the IT infrastructure on demand.
7. Enables running multiple operating systems.

Types of Virtualization:
1.Application Virtualization.

2.Network Virtualization.

3.Desktop Virtualization.

4.Storage Virtualization.

5.Server Virtualization.

6.Data virtualization.

TYPES OF VIRTUALIZATION

DESKTOP VIRTUALIZATION

APPLICATION VIRTUALIZATION

NETWORK VIRTUALIZATION

STORAGE VIRTUALIZATION
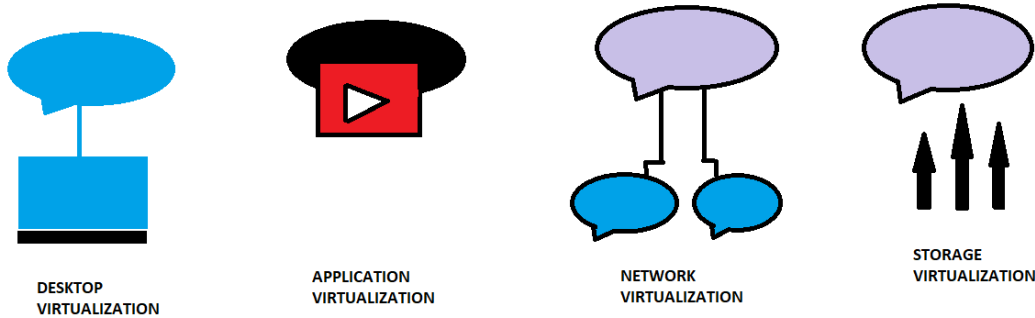
1. Application Virtualization:

Application virtualization helps a user to have remote access of an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet. Example of this would be a user who needs to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

2. Network Virtualization:

The ability to run multiple virtual networks with each has a separate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that potentially confidential to each other. Network virtualization provides a facility to create and provision virtual networks—logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security within days or even in weeks.

3. Desktop Virtualization:

Desktop virtualization allows the users' OS to be remotely stored on a server in the data centre. It allows the user to access their desktop virtually, from any location by a different machine. Users who want specific operating systems other than Windows Server will need to have a virtual desktop. Main benefits of desktop virtualization are user mobility, portability, easy management of software installation, updates, and patches.

4. Storage Virtualization:

Storage virtualization is an array of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is stored, and instead function more like worker bees in a hive. It makes managing storage from multiple sources to be managed and utilized as a single repository. storage virtualization software maintains smooth operations, consistent performance and a continuous suite of advanced functions despite changes, break down and differences in the underlying equipment.

5. Server Virtualization:
This is a kind of virtualization in which masking of server resources takes place. Here, the central-server(physical server) is divided into multiple different virtual servers by changing the identity number, processors. So, each system can operate its own operating systems in isolate manner. Where each sub-server knows the identity of the central server. It causes an increase in the performance and reduces the operating cost by the deployment of main server resources into a sub-server resource. It's beneficial in virtual migration, reduce energy consumption, reduce infrastructural cost, etc.

6. Data virtualization:
This is the kind of virtualization in which the data is collected from various sources and managed that at a single place without knowing more about the technical information like how data is collected, stored & formatted then arranged that data logically so that its virtual view can be accessed by its interested people and stakeholders, and users through the various cloud services remotely. Many big giant companies are providing their services like Oracle, IBM, At scale, Cdata, etc.
 It can be used to performing various kind of tasks such as:

- **Data-integration**
- **Business-integration**
- **Service-oriented architecture data-services**
- **Searching organizational data**

VMware Storage: Understand Your Options
VMware provides a variety of ways for virtual machines to access storage. It supports multiple traditional storage models including SAN, NFS and Fiber Channel (FC), which allow virtualized applications to access storage resources in the same way as they would on a regular physical machine. It also supports Software-Defined Storage (SDS) models that allow you to create and scale elastic pools of storage, and centrally manage data protection and data backup.

Cloud security challenges.

In our technology driven world, security in the cloud is an issue that should be discussed from the board level all the way down to new employees. The CDNetworks blog recently discussed "[what is cloud security](#)" and explained

some of its benefits. Now that we understand what cloud security is, let's take a look at some of the key challenges that may be faced and why you want to prevent unauthorized access at all costs.

Challenge 1: DDoS and Denial-of-Service Attacks

As more and more businesses and operations move to the cloud, cloud providers are becoming a bigger target for malicious attacks. Distributed denial of service (DDoS) attacks are more common than ever before. Verisign reported IT services, cloud platforms (PaaS) and SaaS was the most frequently targeted industry during the first quarter of 2015.

A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a [DDoS attack](#) is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.

Complementing cloud services with [DDoS protection](#) is no longer just good idea for the enterprise; it's a necessity. Websites and web-based applications are core components of 21st century business and require state-of-the-art cybersecurity.

Challenge 2: Data breaches

Known data breaches in the U.S. hit a record-high of 738 in 2014, according to the Identity Theft Research Center, and hacking was (by far) the number one cause. That's an incredible statistic and only emphasizes the growing challenge to secure sensitive data.

Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in all scenarios including private cloud, public cloud, and hybrid cloud situations), some of those security controls are relinquished to a

trusted partner meaning cloud infrastructure can increase security risks. Choosing the right vendor, with a strong record of implementing strong security measures, is vital to overcoming this challenge.

Challenge 3: Data loss

When business critical information is moved into the cloud, it's understandable to be concerned with its security. Losing cloud data, either through accidental deletion and human error, malicious tampering including the installation of malware (i.e. DDoS), or an act of nature that brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.

To face this challenge, it's imperative to ensure there is a disaster recovery process in place, as well as an integrated system to mitigate malicious cyberattacks. In addition, protecting every network layer, including the application layer (layer 7), should be built-in to a cloud security solution.

Challenge 4: Insecure access control points

One of the great benefits of the cloud is it can be accessed from anywhere and from any device. But, what if the interfaces and particularly the application programming interfaces (APIs) users interact with aren't secure? Hackers can find and gain access to these types of vulnerabilities and exploit authentication via APIs if given enough time.
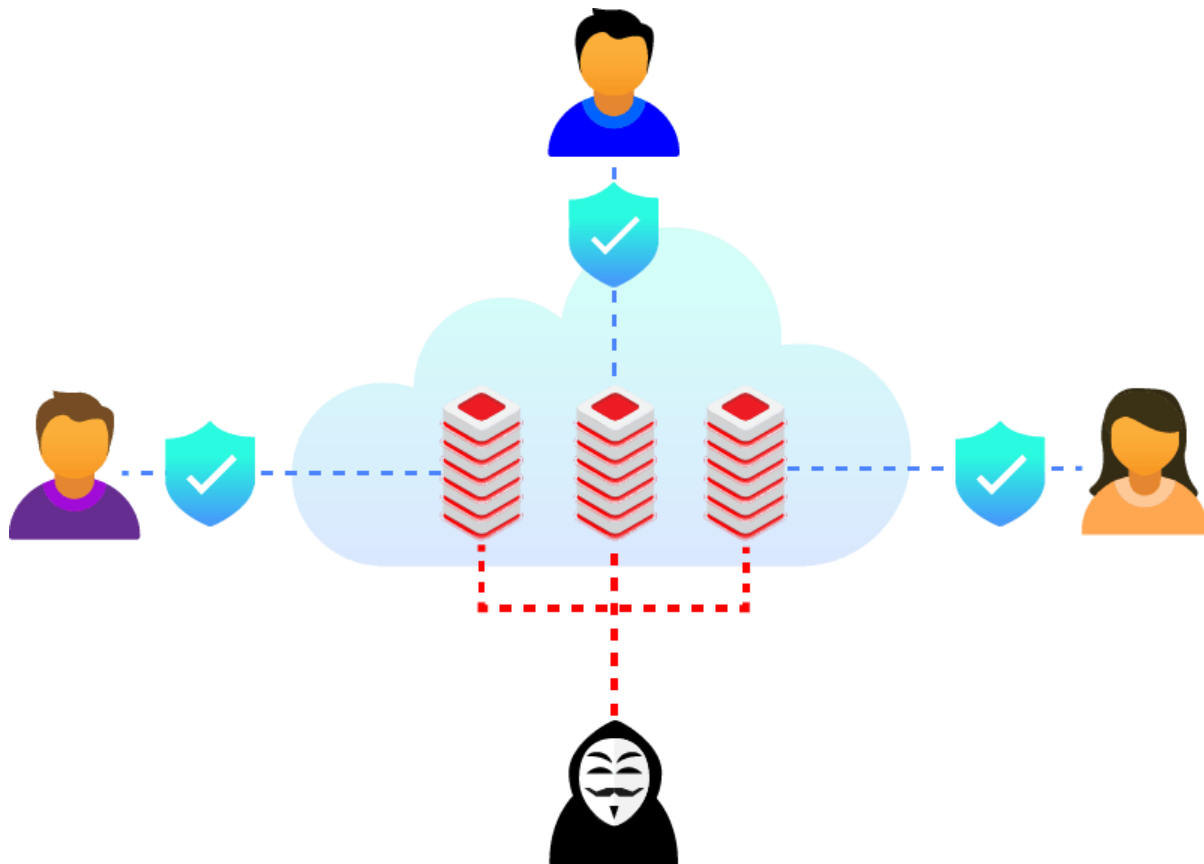
A behavioral [web application firewall](#) examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications and APIS from security breaches within cloud environments and data centers that are not on-premises.

Challenge 5: Notifications and alerts

Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud computing security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough data security and access management plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

Final Thoughts on Cloud Security Challenges

Cloud computing security issues and challenges are not insurmountable. With the right cloud service provider (CSP), technology, and forethought, enterprises can leverage the benefits of cloud technology.

CDNetworks' cloud security solution integrates web performance with the latest in cloud security technology. With 160 points of presence, websites and cloud applications are accelerated on a global scale and, with our cloud security, our clients' cloud-based assets are protected with 24/7 end to end security, including DDoS mitigation at the network and application levels.