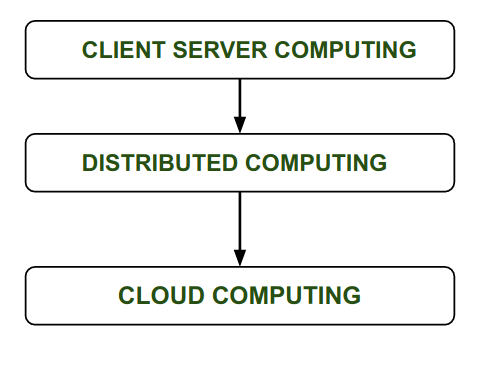
**Chapter-1 Introduction of Cloud Computing**

**Definition:**Cloud computing is defined as the use of hosted services, such as data storage, servers, databases, networking, and software over the internet**. The data is stored on physical servers, which are maintained by a cloud service provider. Computer system resources, especially data storage and computing power, are available on-demand, without direct management by the user in cloud computing.**

 The services hosted on cloud can be broadly divided into infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Based on the deployment model, cloud can also be classified as public, private, and hybrid cloud.Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

**History of Cloud Computing**

* Before Computing was come into existence, client Server Architecture was used where all the data and control of client resides in Server side. If a single user want to access some data, firstly user need to connect to the server and after that user will get appropriate access. But it has many disadvantages. So, After Client Server computing, Distributed Computing was come into existence, in this type of computing all computers are networked together with the help of this, user can share their resources when needed. It also has certain limitations. So in order to remove limitations faced in distributed system, cloud computing was emerged.



* During 1961, John MacCharty delivered his speech at MIT that “Computing Can be sold as a Utility, like Water and Electricity.” According to John MacCharty it was a brilliant idea. But people at that time don’t want to adopt this technology. They thought the technology they are using efficient enough for them.  So, this concept of computing was not appreciated much so and very less will research on it. But as the time fleet the technology caught the idea after few years this idea is implemented. So, this is implemented by Salesforce.com in 1999.
* This company started delivering an enterprise application over the internet and this way the boom of Cloud Computing was started.
* In 2002, Amazon started Amazon Web Services (AWS), Amazon will provide storage, computation over the internet. In 2006 Amazon will launch Elastic Compute Cloud Commercial Service which is open for Everybody to use.
* After that in 2009, Google Play also started providing Cloud Computing Enterprise Application as other companies will see the emergence of cloud Computing they also started providing their cloud services. Thus, in 2009, Microsoft launch Microsoft Azure and after that other companies like Alibaba, IBM, Oracle, HP also introduces their Cloud Services. In today the Cloud Computing become very popular and important skill.

**Advantages :**

* It is easier to get backup in cloud.
* It allows us easy and quick access stored information anywhere and anytime.
* It allows us to access data via mobile.
* It reduces both hardware ad Software cost, and it is easily maintainable.
* One of the biggest advantage of Cloud Computing is Database Security.

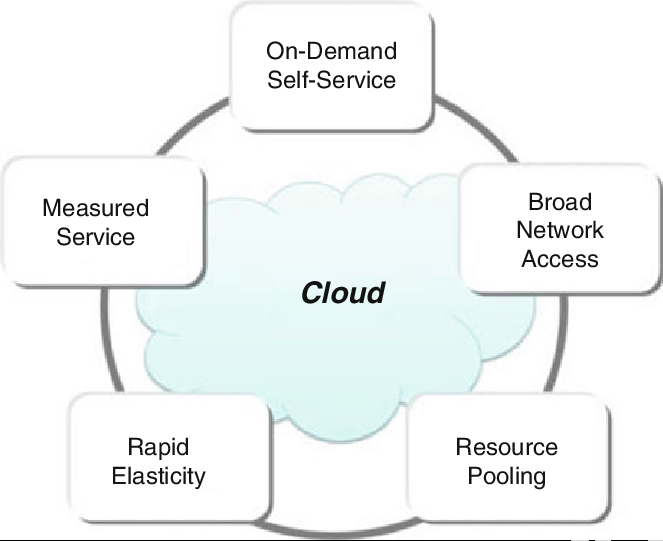
**Disadvantages :**

* It requires good internet connection.
* User have limited control on the data.

**Characteristics of Cloud Computing:**

here are many characteristics of [Cloud Computing](https://www.geeksforgeeks.org/cloud-computing/) here are few of them :

1. **On-demand self-services:** The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.
2. **Broad network access:** The Computing services are generally provided over standard networks and heterogeneous devices.
3. **Rapid elasticity:** The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.
4. **Resource pooling:** The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.
5. **Measured service:** The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.
6. **Multi-tenancy:** Cloud computing providers can support multiple tenants (users or organizations) on a single set of shared resources.
7. **Virtualization:** Cloud computing providers use virtualization technology to abstract underlying hardware resources and present them as logical resources to users.
8. **Resilient computing:**Cloud computing services are typically designed with redundancy and fault tolerance in mind, which ensures high availability and reliability.
9. **Flexible pricing models:**Cloud providers offer a variety of pricing models, including pay-per-use, subscription-based, and spot pricing, allowing users to choose the option that best suits their needs.
10. **Security:** Cloud providers invest heavily in security measures to protect their users’ data and ensure the privacy of sensitive information.
11. **Automation:** Cloud computing services are often highly automated, allowing users to deploy and manage resources with minimal manual intervention.
12. **Sustainability:** Cloud providers are increasingly focused on sustainable practices, such as energy-efficient data centers and the use of renewable energy sources, to reduce their environmental impact.

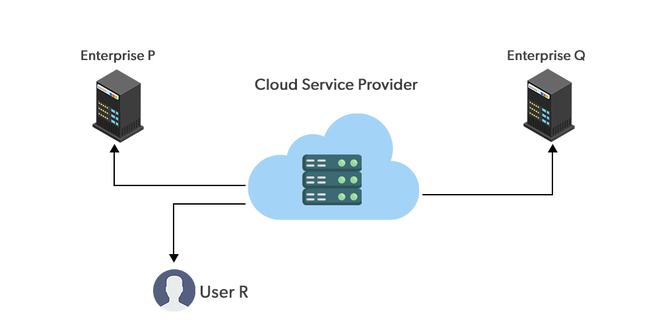


**Cloud Computing Types:**

1. **Public cloud:**

Public clouds are managed by third parties which provide cloud services over the internet to the public, these services are available as pay-as-you-go billing models.

Public clouds are the go-to option for small enterprises, which can start their businesses without large upfront investments by completely relying on public infrastructure for their IT needs. The fundamental characteristics of public clouds are **multitenancy**. A public cloud is meant to serve multiple users, not a single customer.



### **Advantages of using a Public  cloud are:**

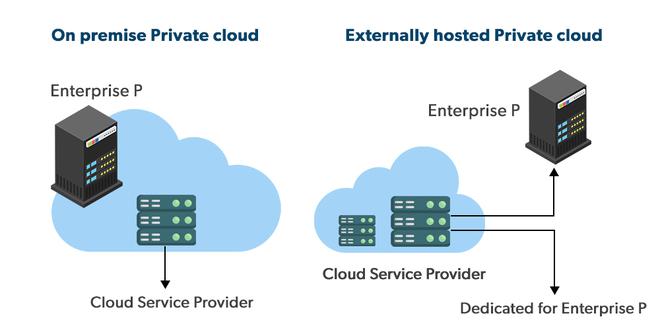
1. High Scalability
2. Cost Reduction
3. Reliability and flexibility
4. Disaster Recovery

### **Disadvantages of using a Public  cloud are:**

1. Loss of control over data
2. Data security and privacy
3. Limited Visibility
4. Unpredictable cos

1. **Private cloud:**

Private clouds are distributed systems that work on private infrastructure and provide the users with dynamic provisioning of computing resources. Instead of a pay-as-you-go model in private clouds, there could be other schemes that manage the usage of the cloud and proportionally billing of the different departments or sections of an enterprise. Private cloud providers are HP Data Centers, Ubuntu, Elastic-Private cloud, Microsoft, etc.



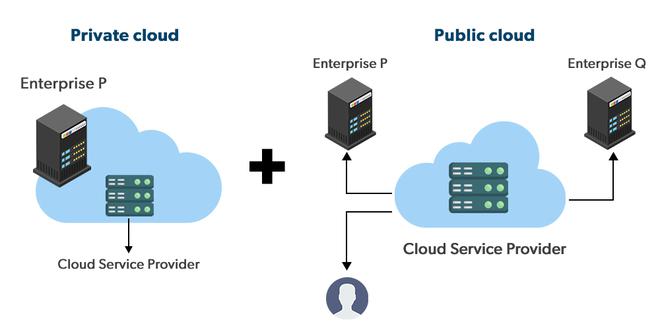
### **The advantages** :

1. **Customer information protection:** In the private cloud security concerns are less since customer data and other sensitive information do not flow out of private infrastructure.
2. **Infrastructure ensuring SLAs:** Private cloud provides specific operations such as appropriate clustering, data replication, system monitoring, and maintenance, disaster recovery, and other uptime services.
3. **Compliance with standard procedures and operations:** Specific procedures have to be put in place when deploying and executing applications according to third-party compliance standards. This is not possible in the case of the public cloud.

**Disadvantages**

1. **The restricted area of operations:** Private cloud is accessible within a particular area. So the area of accessibility is restricted.
2. **Expertise requires:**In the private cloud security concerns are less since customer data and other sensitive information do not flow out of private infrastructure. Hence skilled people are required to manage & operate cloud services.
3. **Hybrid cloud:**

A hybrid cloud is a heterogeneous distributed system formed by combining facilities of the public cloud and private cloud. For this reason, they are also called **heterogeneous clouds.**   
A major drawback of private deployments is the inability to scale on-demand and efficiently address peak loads. Here public clouds are needed. Hence, a hybrid cloud takes advantage of both public and private clouds.



### **Advantages :**

**1) Cost:**Available at a cheap cost than other clouds because it is formed by a distributed system.

**2) Speed:**It is efficiently fast with lower cost, It reduces the latency of the data transfer process.

**3) Security:**Most important thing is security. A hybrid cloud is totally safe and secure because it works on the distributed system network.

### **Disadvantages**

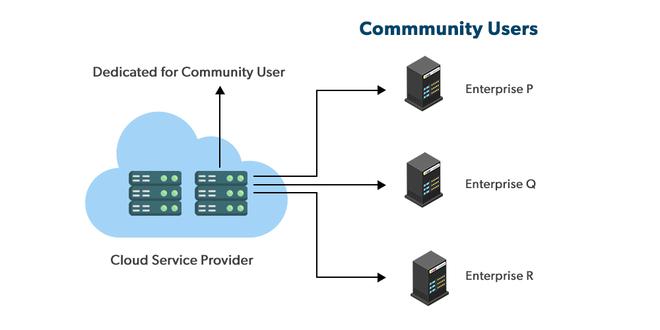
### It’s possible that businesses lack the internal knowledge necessary to create such a hybrid environment. Managing security may also be more challenging. Different access levels and security considerations may apply in each environment.

1. Managing a hybrid cloud may be more difficult. With all of the alternatives and choices available today, not to mention the new PaaS components and technologies that will be released every day going forward, public cloud and migration to public cloud are already complicated enough. It could just feel like a step too far to include hybrid.
2. **Community cloud**

Community clouds are distributed systems created by integrating the services of different clouds to address the specific needs of an industry, a community, or a business sector. But sharing responsibilities among the organizations is difficult.

In the community cloud, the infrastructure is shared between organizations that have shared concerns or tasks. An organization or a third party may manage the cloud.

**`**



### **Advantages**

1. Because the entire cloud is shared by numerous enterprises or a community, community clouds are cost-effective.
2. Because it works with every user, the community cloud is adaptable and scalable. Users can alter the documents according to their needs and requirements.
3. Public cloud is less secure than the community cloud, which is more secure than private cloud.
4. Thanks to community clouds, we may share cloud resources, infrastructure, and other capabilities between different enterprises.

### **Disadvantages**

### **1.** Not all businesses should choose community cloud.

2. gradual adoption of data

3. It’s challenging for corporations to share duties.

### **Differences between Public Cloud and Private Cloud is as follows:**

| **Public Cloud** | **Private Cloud** |
| --- | --- |
| Cloud Computing infrastructure is shared with the public by service providers over the internet. It supports multiple customers i.e, enterprises. | Cloud Computing infrastructure is shared with private organizations by service providers over the internet. It supports one enterprise. |
| Multi-Tenancy i.e, Data of many enterprises are stored in a shared environment but are isolated. Data is shared as per rule, permission, and security. | Single Tenancy i.e, Data of a single enterprise is stored. |
| Cloud service provider provides all the possible services and hardware as the user-base is the world. Different people and organizations may need different services and hardware. Services provided must be versatile. | Specific services and hardware as per the need of the enterprise are available in a private cloud. |
| It is hosted at the Service Provider site. | It is hosted at the Service Provider site or enterprise. |
| It is connected to the public internet. | It only supports connectivity over the private network. |
| Scalability is very high, and reliability is moderate. | Scalability is limited, and reliability is very high. |
| Cloud service provider manages the cloud and customers use them. | Managed and used by a single enterprise. |
| It is cheaper than the private cloud. | It is costlier than the public cloud. |
| Security matters and dependent on the service provider. | It gives a high class of security. |
| Performance is low to medium. | Performance is high. |
| It has shared servers. | It has dedicated servers. |
| Example: Amazon web service (AWS) and Google AppEngine etc. | Example: Microsoft KVM, HP, Red Hat & VMWare etc. |

## Difference between Public Cloud vs Private Cloud vs Hybrid Cloud

| **Factors** | **Public Cloud** | **Private Cloud** | **Hybrid Cloud** |
| --- | --- | --- | --- |
| Resources | Resources are shared among multiple customers | Resources are shared with a single organization | It is a  combination of public and private clouds. based on the requirement. |
| Tenancy | Data of multiple organizations is stored in the public cloud | Data of a single organization is stored in a clouds the public cloud | Data is stored in the public cloud, and provide security in the public cloud. |
| Pay Model | Pay what you used | Have a variety of pricing models | It can include a mix of public cloud pay-as-you-go pricing, and private cloud fixed pricing. It has other pricing models such as consumption-based, subscription-based, etc. |
| Operated by | Third-party service provider | Specific  organization | Can be a combination of both |
| Scalability and Flexibility | It has more scalability and flexibility, | It has predictability and consistency | It has scalability and flexibility by allowing organizations to use a combination of public and private cloud services. |
| Expensive | less expensive | More expensive | Can be more expensive, but it can also be less expensive , depending on the specific needs and requirements of the organization. |
| Availability | The general public (over the internet) | Restricted to a specific organization | Can be a combination of both. |

**Issues of Cloud Computing:**

These are major issues in Cloud Computing:

**1. Privacy:** The user data can be accessed by the host company with or without permission. The service provider may access the data that is on the cloud at any point in time. They could accidentally or deliberately alter or even delete information.

**2. Compliance:** There are many regulations in places related to data and hosting. To comply with regulations the user may have to adopt deployment modes that are expensive.

**3. Security:** Cloud-based services involve third-party for storage and security. Can one assume that a cloud-based company will protect and secure one’s data if one is using their services at a very low or for free? They may share users’ information with others. Security presents a real threat to the cloud.

**4.Higher Cost:**If you want to use cloud services uninterruptedly then you need to have a powerful network with higher bandwidth than ordinary internet networks, and also if your organization is broad and large so ordinary cloud service subscription won’t suit your organization. Otherwise, you might face hassle in utilizing an ordinary cloud service while working on complex projects and applications. This is a major problem before small organizations, that restricts them from diving into cloud technology for their business.

**5.Recovery of lost data in contingency:**Before subscribing any cloud service provider goes through all norms and documentations and check whether their services match your requirements and sufficient well-maintained resource infrastructure with proper upkeeping. Once you subscribed to the service you almost hand over your data into the hands of a third party. If you are able to choose proper cloud service then in the future you don’t need to worry about the recovery of lost data in any contingency.

**6. Upkeeping(management) of Cloud:**Maintaining a cloud is a herculin task because a cloud architecture contains a large resources infrastructure and other challenges and risks as well, user satisfaction, etc. As users usually pay for how much they have consumed the resources. So, sometimes it becomes hard to decide how much should be charged in case the user wants scalability and extend the services.

**7. Lack of resources/skilled expertise:**One of the major issues that companies and enterprises are going through today is the lack of resources and skilled employees. Every second organization is seeming interested or has already been moved to cloud services. That’s why the workload in the cloud is increasing so the cloud service hosting companies need continuous rapid advancement. Due to these factors, organizations are having a tough time keeping up to date with the tools. As new tools and technologies are emerging every day so more skilled/trained employees need to grow. These challenges can only be minimized through additional training of IT and development staff.

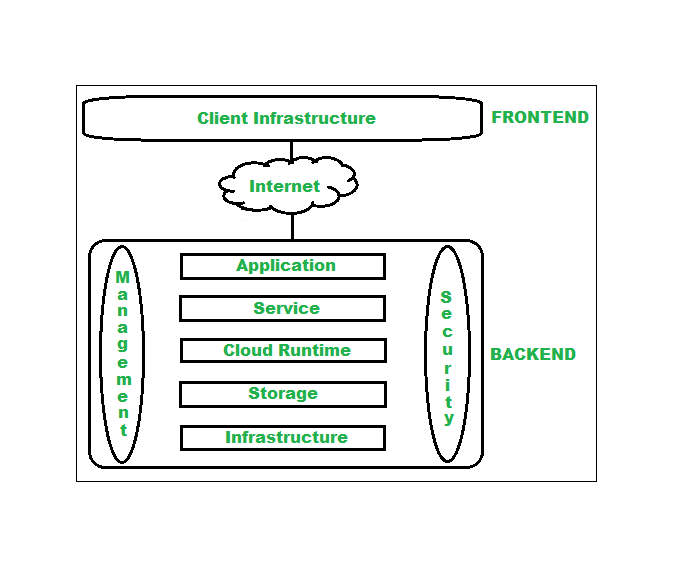
**\**

**Chapter-2**

**Cloud Architecture- Services and Models**

**Cloud Computing Architecture :**  
The cloud architecture is divided into 2 parts i.e.

1. Frontend
2. Backend

****

Architecture of cloud computing is the combination of both [SOA (Service Oriented Architecture)](https://www.geeksforgeeks.org/service-oriented-architecture/) and EDA (Event Driven Architecture). Client infrastructure, application, service, runtime cloud, storage, infrastructure, management and security all these are the components of cloud computing architecture.

**1. Frontend :**  
Frontend of the cloud architecture refers to the client side of cloud computing system. Means it contains all the user interfaces and applications which are used by the client to access the cloud computing services/resources. For example, use of a web browser to access the cloud platform.

* **Client Infrastructure –** Client Infrastructure is a part of the frontend component. It contains the applications and user interfaces which are required to access the cloud platform.
* In other words, it provides a GUI( Graphical User Interface ) to interact with the cloud.

**2. Backend :**  
Backend refers to the cloud itself which is used by the service provider. It contains the resources as well as manages the resources and provides security mechanisms. Along with this, it includes huge storage, virtual applications, virtual machines, traffic control mechanisms, deployment models, etc.

1. **Application –**  
   Application in backend refers to a software or platform to which client accesses. Means it provides the service in backend as per the client requirement.
2. **Service –**  
   Service in backend refers to the major three types of cloud based services like [SaaS, PaaS and IaaS](https://www.geeksforgeeks.org/cloud-based-services/). Also manages which type of service the user accesses.
3. **Runtime Cloud-**  
   Runtime cloud in backend provides the execution and Runtime platform/environment to the Virtual machine.
4. **Storage –**  
   Storage in backend provides flexible and scalable storage service and management of stored data.
5. **Infrastructure –**  
   Cloud Infrastructure in backend refers to the hardware and software components of cloud like it includes servers, storage, network devices, virtualization software etc.
6. **Management –**  
   Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.
7. **Security –**  
   Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, and infrastructure to end-users.
8. **Internet –**  
   Internet connection acts as the medium or a bridge between frontend and backend and establishes the interaction and communication between frontend and backend.
9. **Database**– Database in backend refers to provide database for storing structured data, such as SQL and NOSQL databases. Example of Databases services include Amazon RDS, Microsoft Azure SQL database and Google CLoud SQL.
10. **Networking**– Networking in backend services that provide networking infrastructure for application in the cloud, such as load balancing, DNS and virtual private networks.
11. **Analytics**– Analytics in backend service that provides analytics capabillities for data in the cloud, such as warehousing, bussness intellegence and machine learning.

**Benefits of Cloud Computing Architecture :**

* Makes overall cloud computing system simpler.
* Improves data processing requirements.
* Helps in providing high security.
* Makes it more modularized.
* Results in better disaster recovery.
* Gives good user accessibility.
* Reduces IT operating costs.
* Provides high level reliability.
* Scalability.

**Cloud computing services:**

Most cloud computing services fall into five broad categories:

1. Software as a service (SaaS)
2. Platform as a service (PaaS)
3. Infrastructure as a service (IaaS)
4. Anything/Everything as a service (XaaS)
5. Function as a Service (FaaS)

**1. Software as a service (SaaS)**

[Software-as-a-Service (SaaS)](https://www.geeksforgeeks.org/software-as-a-service-saas/) is a way of delivering services and applications over the Internet. Instead of installing and maintaining software, we simply access it via the Internet, freeing ourselves from the complex software and hardware management. It removes the need to install and run applications on our own computers or in the data centers eliminating the expenses of hardware as well as software maintenance.   
SaaS provides a complete software solution that you purchase on a **pay-as-you-go** basis from a cloud service provider. Most SaaS applications can be run directly from a web browser without any downloads or installations required. The SaaS applications are sometimes called **Web-based software, on-demand software, or hosted software.**

#### **Advantages of SaaS**

1. **Cost-Effective:** Pay only for what you use.
2. **Reduced time:** Users can run most SaaS apps directly from their web browser without needing to download and install any software. This reduces the time spent in installation and configuration and can reduce the issues that can get in the way of the software deployment.
3. **Accessibility:** We can Access app data from anywhere.
4. **Automatic updates:** Rather than purchasing new software, customers rely on a SaaS provider to automatically perform the updates.
5. **Scalability:**It allows the users to access the services and features on-demand.

The various companies providing *Software as a service* are Cloud9 Analytics, Salesforce.com, Cloud Switch, Microsoft Office 365, Big Commerce, Eloqua, dropBox, and Cloud Tran.

**Disadvantages of Saas :**

1. **Limited customization**: SaaS solutions are typically not as customizable as on-premises software, meaning that users may have to work within the constraints of the SaaS provider’s platform and may not be able to tailor the software to their specific needs.
2. **Dependence on internet connectivity**: SaaS solutions are typically cloud-based, which means that they require a stable internet connection to function properly. This can be problematic for users in areas with poor connectivity or for those who need to access the software in offline environments.
3. **Security concerns:** SaaS providers are responsible for maintaining the security of the data stored on their servers, but there is still a risk of data breaches or other security incidents.
4. **Limited control over data:** SaaS providers may have access to a user’s data, which can be a concern for organizations that need to maintain strict control over their data for regulatory or other reasons.

**2. Platform as a Service**

[PaaS](https://www.geeksforgeeks.org/platform-as-a-service-paas-and-its-types/) is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser.   
A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.

#### **Advantages of PaaS:**

1. **Simple and convenient for users:**It provides much of the infrastructure and other IT services, which users can access anywhere via a web browser.
2. **Cost-Effective:**It charges for the services provided on a per-use basis thus eliminating the expenses one may have for on-premises hardware and software.
3. **Efficiently managing the lifecycle:** It is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.
4. **Efficiency:** It allows for higher-level programming with reduced complexity thus, the overall development of the application can be more effective.

The various companies providing *Platform as a service* are Amazon Web services Elastic Beanstalk, Salesforce, Windows Azure, Google App Engine, cloud Bees and IBM smart cloud.

**Disadvantages of Paas:**

1. **Limited control over infrastructure:** PaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.
2. **Dependence on the provider**: Users are dependent on the PaaS provider for the availability, scalability, and reliability of the platform, which can be a risk if the provider experiences outages or other issues.
3. **Limited flexibility:** PaaS solutions may not be able to accommodate certain types of workloads or applications, which can limit the value of the solution for certain organizations.

**3. Infrastructure as a Service**

Infrastructure as a service (IaaS) is a service model that delivers computer infrastructure on an outsourced basis to support various operations. Typically IaaS is a service where infrastructure is provided as outsourcing to enterprises such as networking equipment, devices, database, and web servers.   
It is also known as **Hardware as a Service (HaaS).** IaaS customers pay on a per-user basis, typically by the hour, week, or month.

#### **Advantages of IaaS:**

1. **Cost-Effective:** Eliminates capital expense and reduces ongoing cost and IaaS customers pay on a per-user basis, typically by the hour, week, or month.
2. **Website hosting:** Running websites using IaaS can be less expensive than traditional web hosting.
3. **Security:**The IaaS Cloud Provider may provide better security than your existing software.
4. **Maintenance:** There is no need to manage the underlying data center or the introduction of new releases of the development or underlying software. This is all handled by the IaaS Cloud Provider.

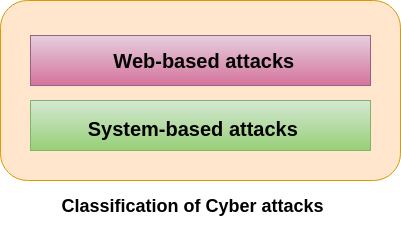
The various companies providing *Infrastructure as a service* are [Amazon web services](https://www.geeksforgeeks.org/amazon-web-services-setting-up-an-aws-account/), Bluestack, IBM, Openstack, Rackspace, and Vmware.

**Disadvantages of laaS :**

1. **Limited control over infrastructure:**IaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.
2. **Security concerns**: Users are responsible for securing their own data and applications, which can be a significant undertaking.
3. **Limited access:**Cloud computing may not be accessible in certain regions and countries due to legal policies.

**Chapter-4**

**Types of Attack:** Cyber-attacks can be classified into the following categories:



## **Web-based attacks**

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

**1. Injection attacks**

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

**Example-** SQL Injection, code Injection, log Injection, XML Injection etc.

**2. DNS Spoofing**

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

**3. Session Hijacking**

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

**4. Phishing**

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

**5. Brute force**

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

**6. Denial of Service**

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

**Volume-based attacks-** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

**Protocol attacks-** It consumes actual server resources, and is measured in a packet.

**Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

**7. Dictionary attacks**

This type of attack stored the list of a commonly used password and validated them to get original password.

**8. URL Interpretation**

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

**9. File Inclusion attacks**

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

**10. Man in the middle attacks**

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

## **System-based attacks**

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

**1. Virus**

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

**2. Worm**

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

**3. Trojan horse**

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

**4. Backdoors**

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

**5. Bots**

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

## **What is Network Security?**

In other words, Network security is defined as the activity created to protect the integrity of your network and data.

Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

Network security uses several layers of protection, both at the edge of the network and within it. Each layer has rules and controls that determine who can access network resources. People who are allowed access can use the network safely, but those who try to harm it with attacks or other threats are stopped from doing so.

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data. These levels are:

* **Physical Network Security:**This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. The same can be achieved by using devices like biometric systems.
* **Technical Network Security:** It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.
* **Administrative Network Security:** This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

## **Types of Network Security**

Here below are some important types of network security:

### **Email Security**

Email Security is defined as the process designed to protect the Email Account and its contents safe from unauthorized access. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.

To stop critical data from being lost, an email security programme restricts outgoing messages and stops incoming threats.

### **Network Segmentation**

Network traffic is divided into several categories by software-defined segmentation, which also facilitates the enforcement of security regulations. Ideally, endpoint identity—rather than just IP addresses—is the basis for the classifications. To ensure that the appropriate amount of access is granted to the appropriate individuals and that suspicious devices are controlled and remediated, access permissions can be assigned based on role, location, and other factors.

### **Access Control**

Your network should not be accessible to every user. You need to identify every user and every device in order to keep out any attackers. You can then put your security policies into effect. Noncompliant endpoint devices might either have their access restricted or blocked.

### **Sandboxing**

[Sandboxing](https://www.geeksforgeeks.org/sandbox-security-model/) is a cybersecurity technique in which files are opened or code is performed on a host computer that simulates end-user operating environments in a secure, isolated environment. To keep threats off the network, sandboxing watches the code or files as they are opened and searches for harmful activity.

### **Cloud Network Security**

This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized (ख़तरे में डालना) by anything. Many businesses embrace(अपनाना)  [SaaS applications](https://www.geeksforgeeks.org/cloud-based-services) for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

### **Web Security**

A online security solution will restrict access to harmful websites, stop web-based risks, and manage staff internet usage. Your web gateway will be safeguarded both locally and in the cloud. “[Web security](https://www.geeksforgeeks.org/web-security-considerations/)” also include the precautions you take to safeguard your personal website.

### **Intrusion Prevention System(IPS)**

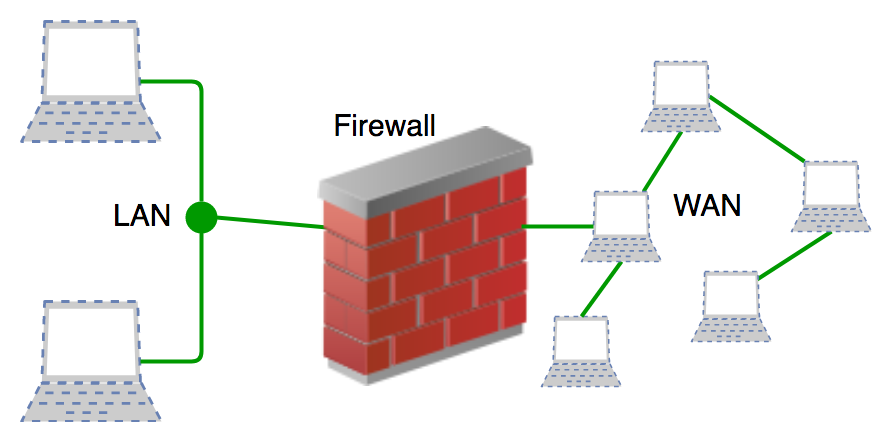
An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

### **Antivirus and Anti-malware Software**

This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like [Viruses, Trojans, and Worms](https://www.geeksforgeeks.org/malware-and-its-types) is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.

### **Firewalls Security**

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by [Access Control Lists](https://www.geeksforgeeks.org/access-lists-acl/) (ACLs) residing on routers.



### **Application Security**

Application security denotes the security precautionary measures utilized at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever.

### **Wireless Security**

[Wireless networks](https://www.geeksforgeeks.org/wired-and-wireless-networking/) are less secure than wired ones. If not properly secured, setting up a wireless LAN can be like having Ethernet ports available everywhere, even in places like parking lots. To prevent attacks and keep your wireless network safe, you need dedicated products designed to protect it from exploits and unauthorized access.

### **Mobile Device Security**

Cybercriminals are focusing more on mobile devices and apps. In the next three years, about 90 percent of IT organizations might allow corporate applications on personal mobile devices. It’s crucial to control which devices can connect to your network and set up their connections securely to protect network traffic from unauthorized access.

### **VPN Security**

A virtual private network (VPN) encrypts the connection between a device and a network, usually over the internet. A remote-access VPN commonly uses IPsec or[Secure Sockets Layer](https://www.geeksforgeeks.org/secure-socket-layer-ssl/)(SSL) to verify and secure the communication between the device and the network. This encryption ensures that data transmitted between the device and the network remains private and secure from unauthorized access.

## **Benefits of Network Security**

Network Security has several benefits, some of which are mentioned below:

* Network Security helps in protecting clients’ information and data which ensures reliable access and helps in protecting the data from cyber threats.
* Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.
* It overall protects the reputation of the organization as it protects the data and confidential items.

## **Advantages of Network Security**

* **Protection from Unauthorized Access**: Network security measures such as firewalls and authentication systems prevent unauthorized users from accessing sensitive information or disrupting network operations.
* **Data Confidentiality**: Encryption technologies ensure that data transmitted over the network remains confidential and cannot be intercepted by unauthorized parties.
* **Prevention of Malware and Viruses**: Network security solutions like antivirus software and intrusion detection systems (IDS) detect and block malware, viruses, and other malicious threats before they can infect systems.
* **Secure Remote Access**: [Virtual private networks](https://www.geeksforgeeks.org/what-is-vpn-and-how-it-works/)(VPNs) and other secure remote access methods enable employees to work remotely without compromising the security of the organization’s network and data.

## **Disadvantages of Network Security**

* **Complexity and Management Overhead**: Implementing and managing network security measures such as [firewalls](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/), encryption, and[intrusion detection systems](https://www.geeksforgeeks.org/intrusion-detection-system-ids/) (IDS) can be complex and require specialized knowledge and resources.
* **Cost**: Effective network security often requires investment in hardware, software, and skilled personnel, which can be expensive for organizations, especially smaller ones.
* **Privacy Concerns**: Some network security measures, such as deep packet inspection and monitoring, may raise privacy concerns among users and stakeholders, requiring careful balancing of security needs with individual privacy rights.

**Security stack**

A security stack in cloud computing is a collection of security tools, practices, and protocols designed to protect cloud environments. It typically addresses various aspects of security, including data protection, threat detection, identity management, and compliance. Here are the key components of a comprehensive cloud security stack:

### 1. **Network Security**

* **Firewalls:** Protect against unauthorized access by filtering traffic.
* **Intrusion Detection and Prevention Systems (IDPS):** Monitor and respond to potential threats.
* **Virtual Private Networks (VPNs):** Secure connections for remote access.

### 2. **Data Security**

* **Encryption:** Protect data at rest and in transit using strong encryption protocols.
* **Data Loss Prevention (DLP):** Monitor and protect sensitive data from being leaked or accessed improperly.
* **Backup and Recovery:** Regularly back up data and have a plan for data recovery in case of loss or corruption.

### 3. **Identity and Access Management (IAM)**

* **Multi-Factor Authentication (MFA):** Add an extra layer of security to user logins.
* **Single Sign-On (SSO):** Simplify user authentication while maintaining security.
* **Role-Based Access Control (RBAC):** Ensure users have appropriate access levels based on their roles.

### 4. **Application Security**

* **Secure Development Practices:** Implement secure coding standards and practices.
* **Web Application Firewalls (WAFs):** Protect web applications from common attacks like SQL injection and cross-site scripting (XSS).
* **API Security:** Protect and monitor API endpoints to prevent unauthorized access.

### 5. **Endpoint Security**

* **Anti-Malware/Anti-Virus:** Protect devices against malware and viruses.
* **Endpoint Detection and Response (EDR):** Provide advanced threat detection and response capabilities on endpoints.

### 6. **Threat Intelligence and Monitoring**

* **Security Information and Event Management (SIEM):** Aggregate and analyze security data from various sources to detect threats.
* **Security Operations Center (SOC):** A dedicated team to monitor, detect, and respond to security incidents.
* **Threat Intelligence Feeds:** Receive updates on the latest threats and vulnerabilities.

### 7. **Compliance and Governance**

* **Compliance Tools:** Ensure adherence to industry standards and regulations (e.g., GDPR, HIPAA, PCI DSS).
* **Audit and Logging:** Maintain logs of all activities for auditing and forensic purposes.
* **Policy Management:** Define and enforce security policies across the organization.

### 8. **Cloud-Specific Security Tools**

* **Cloud Access Security Brokers (CASB):** Monitor and secure data across cloud services.
* **Container Security:** Protect containerized applications and ensure secure container orchestration.
* **Serverless Security:** Implement security measures for serverless architectures.

### 9. **Incident Response and Management**

* **Incident Response Plan:** Have a documented and tested plan for responding to security incidents.
* **Forensic Tools:** Investigate and analyze security incidents to understand their impact and prevent recurrence.

### 10. **Education and Awareness**

* **Security Training:** Regularly train employees on security best practices and threat awareness.
* **Phishing Simulations:** Conduct simulated phishing attacks to test and improve employee readiness.

By integrating these components, organizations can build a robust security stack that protects their cloud environments against a wide range of threats and vulnerabilities

**Gartner’s Seven Cloud Security Risk**

according to analyst firm Gartner, “Cloud computing is fraught with security risks”,

Cloud computing has “unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing,” Gartner says.

Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor.

1. **Privileged user access**. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the “physical, logical and personnel controls” IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. “Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access,” Gartner says.

2**. Regulatory compliance**. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are “signaling that customers can only use them for the most trivial functions,” according to Gartner.

**3. Data location.** When you use the cloud, you probably won’t know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

**4. Data segregation**. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn’t a cure-all. “Find out what is done to segregate data at rest,” Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. “Encryption accidents can make data totally unusable, and even normal encryption can complicate availability,” Gartner says.

**5. Recovery.** Even if you don’t know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. “Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure,” Gartner says. Ask your provider if it has “the ability to do a complete restoration, and how long it will take.”

**6. Investigative support**. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. “Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.”

**7. Long-term viability**. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. “Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application,” Gartner says.

**Security Issues int cloud computing**:  
There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

1. **Data Loss –**  
   Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage.  As we know that our sensitive data is in the hands of Somebody else, and we don’t have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.
2. **Interference of Hackers and Insecure API’s –**  
   As we know, if we are talking about the cloud and its services it means we are talking about the Internet.  Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface’s and API’s which are used by an external user. But also in cloud computing, few services are available in the public domain which are the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.
3. **User Account Hijacking –**  
   Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by a hacker then the hacker has full authority to perform Unauthorized Activities**.**
4. **Changing Service Provider –**  
   Vendor lock-In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from[AWS Cloud](https://www.geeksforgeeks.org/introduction-to-amazon-web-services/) to [Google Cloud](https://www.geeksforgeeks.org/what-is-google-cloud-platform-gcp/) Services then they face various problems like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of [AWS](https://www.geeksforgeeks.org/introduction-to-aws-simple-storage-service-aws-s3/)are different from Google Cloud, etc.
5. **Lack of Skill –**   
   While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Companies who doesn’t have skilled Employees. So it requires a skilled person to work with Cloud Computing.
6. **Denial of Service (DoS) attack –**   
   This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost.  So, in order to recover data, it requires a great amount of money as well as time to handle it.
7. **Shared Resources:** Cloud computing relies on a shared infrastructure. If one customer’s data or applications are compromised, it may potentially affect other customers sharing the same resources, leading to a breach of confidentiality or integrity.
8. **Compliance and Legal Issues:** Different industries and regions have specific regulatory requirements for data handling and storage. Ensuring compliance with these regulations can be challenging when data is stored in a cloud environment that may span multiple jurisdictions.
9. **Data Encryption:**While data in transit is often encrypted, data at rest can be susceptible to breaches. It’s crucial to ensure that data stored in the cloud is properly encrypted to prevent unauthorized access.
10. **Insider Threats:** Employees or service providers with access to cloud systems may misuse their privileges, intentionally or unintentionally causing data breaches. Proper access controls and monitoring are essential to mitigate these threats.
11. **Data Location and Sovereignty:**Knowing where your data physically resides is important for compliance and security. Some cloud providers store data in multiple locations globally, and this may raise concerns about data sovereignty and who has access to it.
12. **Loss of Control:**When using a cloud service, you are entrusting a third party with your data and applications. This loss of direct control can lead to concerns about data ownership, access, and availability.
13. **Incident Response and Forensics:**Investigating security incidents in a cloud environment can be complex. Understanding what happened and who is responsible can be challenging due to the distributed and shared nature of cloud services.
14. **Data Backup and Recovery:** Relying on cloud providers for data backup and recovery can be risky. It’s essential to have a robust backup and recovery strategy in place to ensure data availability in case of outages or data loss.
15. **Social Engineering and Phishing:** Attackers may use social engineering tactics to trick users or cloud service providers into revealing sensitive information or granting unauthorized access.