What is a Public Cloud?

Public Cloud is an IT model where on-demand computing services and infrastructure are managed by a third-party provider and shared with multiple organizations using the public Internet. Public cloud service providers may offer cloud-based services such as infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (Saas) to users for either a monthly or pay-per-use fee, eliminating the need for users to host these services on site in their own data center.

Cloud service providers use groups of data centers that are partitioned into virtual machines and shared by tenants. Tenants may simply rent the use of those virtual machines, or they may pay for additional cloud-based services such as software applications, application development tools, or storage. Companies often use public cloud services for less-sensitive applications that have unpredictable spikes in usage or for storing data that does not require frequent access.

Public cloud makes computing resources available to anyone for purchase. Multiple users typically share the use of a public cloud. In contrast, private cloud involves cloud-based services that are hosted within an organization's own private servers.

Why Public Cloud?

Many enterprise businesses look to the public cloud as a way to scale existing IT resources on demand without committing to expanding their physical IT infrastructure. For instance, instead of purchasing a physical desktop machine, a company can purchase a virtual desktop license. The virtual desktop can be spun up or deactivated in minutes and can be located anywhere, instantly.
The public cloud is also a popular solution for storage needs since data stored on a public cloud is backed up and accessible from anywhere. There are many different types of storage plans, and data that does not need to be accessed frequently can often be stored in the public cloud very cheaply.
For companies that host an application with periods of peak usage, the public cloud makes perfect sense because the extra computing power is only needed for a short time.

Using the public cloud can save businesses money in a couple of different ways:

Lower equipment purchase costs: Because employees can access and pay for cloud-based resources only when they need them, using public cloud-based desktops and applications is often less expensive than purchasing physical IT equipment or software packages that may or may not be used and will need to be maintained.

Lower equipment maintenance costs: With public cloud-based services, the cost of maintaining IT equipment is also passed on to the cloud service provider.
A small or new business may have an easier time migrating applications to the public cloud; organizations with a large legacy IT infrastructure and applications have more to consider and plan for. However, more and more enterprise businesses are moving toward the public cloud as one element of a multi-faceted IT plan. This way, they can access the benefits of the public cloud while also maintaining the different benefits that come with on-premises architecture and private cloud options.

Advantages of Public Cloud

1. **Scalability**

   Public cloud services come with the auto-scaling feature. This means that all the virtual machines present inside the Public cloud system have the capability to get created, scaled, and shut down at an infinite speed. Therefore, ultimately the workload will be balanced according to the needs so that you can avoid downtime and crashes.

2. **Cost**

   Since a third party provides the Public cloud services, there is no need for an IT employee to look after and maintain the system. The cost of bandwidth, hardware, and application is the sole responsibility of the provider. Hence, the initial investment here is almost zero. Moreover, Public cloud services follow the model of pay-as-you-go which means that the payment is made monthly or annually according to the way the resources are being used.

4. **Reliability**

Public cloud services offer greater reliability. This means there are very less chances of failure interrupting your service. The data center present on the network of servers can undergo frequent failure. Even if it does so, it will not be an issue since the workload will be distributed among the remaining data centers.

5. **Data Recovery**

A Disaster recovery plan is generally difficult and complex to deploy. That is the reason why most IT companies don't consider this implementation. However Public cloud has very little risk of losing data here. This is because most of the multiple infrastructures are available in the Public cloud services.

Disadvantages\ Limitations of Public Cloud

1. Low Security and control
The security and privacy of data present inside a Public cloud service remain a concern for many businesses. The Public cloud services offered by many providers are secure to some extent. But the problem lies within the company and how they are going to use them. Therefore, companies must make use of cyber security practices. And also trust in the third party provider is also questioned since they can be from different countries having their own set of security and privacy regulations.

2. Flexibility
Even though Public cloud services are very flexible in terms of scalability, there are issues with security and configurations. Some Public cloud providers do not grant freedom to install an operating system or switch storage solutions. That is the reason why Public cloud services are not recommended for organizations with compliance regulations.

3. No Control
Using the Public cloud services means that you are sharing the same infrastructure with the other customers. The maintenance and management have been entirely taken care of by the service provider. The users have no control over it.

4. Customization
The atmosphere of the Public cloud service can limit any customization process. Hence, customization of resources or services is almost made impossible in a Public cloud service. This can be disadvantageous, especially to companies with complex network architecture and application processes.

5. Customer Support
Public cloud models lack on the side of customer support. In fact, it is a separate contract for the client. Customer support is an important point to remember since some providers do not deliver quality service. Therefore, users need to discover solutions on their own.

Disadvantages\ Limitations of Public Cloud

6. One-size-fits-all solutions

When you sign up with a public cloud provider, you choose an existing package of services. This generic approach to IT services keeps costs down, but it hasn't been tailored to your business, which could be a nightmare if you've got a complicated network architecture. You'll have the exact same solution as the rest of the cloud customers, with little scope for this to adapt to your business. It might be unable to support your business if your requirements stray too far from the set dimensions of your public cloud.

7. Limited visibility

The view you have of your data will be through whatever portal is provided by your public cloud host. If you want more information than is displayed, there's nothing you can do. While there is probably nothing underhand going on, it's an undeniable disadvantage of the public cloud that you won't have complete visibility on all the metrics of your data storage. We're living in an age of information, and the more data you have, the better equipped you'll be to make business-critical decisions. Being ignorant of certain information is never a part of anyone's IT plan and might leave your business in the dark.

8. Outgrowing the platform

The public cloud is well suited for businesses that are starting out or growing rapidly. But public cloud services are intended to be a flexible alternative to other data storage, so once your IT system grows large enough and your priority is now capacity over flexibility, it's no longer cost-effective to stay on the public cloud. Dropbox reportedly saved nearly $75M over two years by moving off of the public cloud and into colocation services hosting private hardware. You will outgrow your public cloud platform eventually and need to make sure you don't lose out financially by staying on it for too long.

9. Unreliable services

Even the biggest cloud providers still suffer downtime, whether it's Google, Microsoft, or AWS. It's an unavoidable fact of life, but if there's a lack of communication and a slow fix, then that's an unnecessary disruption to your business. Ultimately, it's your IT that matter to your business, so if you're regularly experiencing problems, your provider's overall performance doesn't matter. You need to be able to quickly access the engineers responsible for your systems when something goes wrong, to find a fix as soon as possible. With a large and complicated shared public cloud system, getting to the root of the issue can be a slow process

Disadvantages\ Limitations of Public Cloud

7. Compliance issues

Ever since GDPR came into effect, businesses have been more aware of compliance issues around storing personal or sensitive data. If you work in an industry with a focus on data compliance – like banking, healthcare, or countless others – then this takes on extra importance since you can't let a lack of data compliance lose your business. The lack of control with the public cloud makes it difficult to meet data regulation requirements, which is why a lot of businesses use the private cloud or their own hardware for storing sensitive data.

8. Unpredictable costs

Public cloud services offer a "pay as you go" and "pay for what you use" billing format, which is great for small businesses with variable usage. However, it can cause a nightmare for your accounts department with how unpredictable it is. It's easy to create some extra workload and suddenly be over budget, which can quickly eat into the profits of your business. This is a disadvantage unique to a public cloud since almost all other IT infrastructure solutions will have a set monthly cost.

Is the public cloud right for your business?

Reviewing the pros and cons of the public cloud is essential to understanding if it's a good fit for your business or not. Unfortunately, if your business prioritizes security, has specific IT requirements, or needs to get spending under control, then the public cloud won't be a good fit for you, especially in the long term.

Instead, you could look at a private cloud solution, which still provides a lot of support but with better security and fixed costs. Or you can get the best of both worlds and look at a hybrid IT system, where you can keep the flexibility of your public cloud but combine it with a more secure and reliable IT platform.

The high cost of accessing the public cloud for Long-Term

The actual storage fee for housing your data in the public cloud is typically low. But once your data is in there, you must pay to access it, which for many comes as a surprise. That means the more value you get from your data, the more money you have to pay. Although these charges are considered low (in the range of $0.01 to $0.05 per 1,000 transactions) costs can quickly escalate when a customer is using the public cloud as primary storage or for storing any particularly active data set.

Public cloud vendors also charge for a variety of services besides just storing your data. You need to not only be aware of these costs but also do a cloud storage cost analysis to really understand your costs before moving your data to the public cloud.

Differences

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.

Differences

Public Cloud	Private Cloud
It is hosted at the Service Provider site.	It is hosted at the Service Provider site or enterprise.
organizationsenterprisesIt 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.

Differences

Public Cloud	Private Cloud
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.

Vendor Selection:

HOW TO CHOOSE A CLOUD SERVICE PROVIDER

Cloud computing is still an evolving technology. It marks the transition from you owning the hardware and software to you renting it for your business needs. It's the disruptive technology that's enabling businesses like no other. While the benefits of the cloud model for enterprises are many, moving to the cloud should be a carefully considered decision.

The most critical aspect in this is the Cloud Service Provider. While you can look at the hardware part of cloud as commodity, you have to switch to a view that you are now looking for a Service, and not merely renting boxes. And that can be tricky business. So what are the things to keep in mind when you choose a Cloud Service Provider?

Vendor Selection:

1. CHOOSE AN ENTERPRISE - CLASS CLOUD

A cloud is a cloud. Right? Wrong. A cloud could be set up with a few boxes, with some freeware, in a dingy basement, with an engineer playing the all-round expert. It could also be set up in a fortified data center using state-of-the-art hardware, and tried, tested and benchmarked software, and run by specialized experts. A cloud could be set up in any configuration in between these as well.

So all clouds are not equal.

What would you choose for your business? If your business needs security and uptime, the last thing you need is your cloud service provider battling security breaches and patching freeware bugs or grappling with commodity hardware going bust.

Vendor Selection:

2. OPT FOR MANAGED CLOUD

Do not sign up for a cloud service without asking if it's managed or not. Are you looking for self-service and self-management? Or do you want support, backups and monitoring? What works better for your business: your team trying to remotely manage things; or your service provider running it like clockwork for you?

Cost is one aspect in this equation. You might get a server or two for what looks like a steal. But then the business needs backups, monitoring and management.

And the costs quickly spiral out of control. Sometimes you end up paying 4-5 times of the low-cost servers you signed up for! So don't presume that all clouds are managed. Read the fine print. Check before you sign up for things which are not there in the SLA, and ask for them.

Vendor Selection:

3. LOOK FOR TRANSPARENCY

There are pricing calculators on most large cloud service providers' websites. They look cheap when you are dealing with just a few servers. And as your need for virtual machines increases, so does the complexity of backups, monitoring and management. And then the pricing will not be the forecast you have in mind. Be clear about what your needs are today, and how will they change over time. And estimate all the possible services you might need in a few months. And then take a call. Just going by the lowest price offer of today may not lead to the lowest TCO you are aiming for.

Vendor Selection:

4. GO LOCAL: LATENCY, COMPLIANCE, PRIVACY

How important are these to your business? As government regulations become more stringent, and as end user demand grows with respect to data confidentiality and privacy, companies are moving their applications hosted in a different country back to their own. Many companies do this to improve latency issues as well. Choose a cloud on these parameters as well. So clouds are increasingly going to be local.

Vendor Selection:

5. ASSESS SECURITY

A cloud is likely to be more secure than the security setups that most mid-size and even many large enterprises have on their premises. Internal threats are not given much thought to, in many enterprises.

But not all cloud service providers will deliver the kind of security you probably assume is being given to you. Make sure that you are aware of the firewalls, IDS/IPS and other systems that they have, and the processes they follow to ensure that there are no breaches. Does the service you signed up for give you the protection of an enterprise-class firewall and IDS/IPS, or do you have to pay extra?

Vendor Selection:

6. UNDERSTAND AVAILABILITY

Availability is a much abused word. You will hear numbers being bandied about when it comes to availability. Tier 2,3, 4, and 99.95%, 99.999% and so on. What do they mean? And do you really get what is being promised? How is it being calculated? Is it annual, monthly, or on a rolling basis?

A Tier 3 data center is expected to deliver 99.9982% uptime, which translates to less than 1.6 hours of downtime in a year. Running a data center comes with huge challenges and a managed cloud service provider has to address them to be able to deliver the uptime businesses need. Yet if your business demands zero downtime, it's best to consider having multiple data centers across geographies.

What is cloud migration?

Cloud migration is the process of moving a company's digital assets, services, databases, IT resources, and applications either partially, or wholly, into the cloud. Cloud migration is also about moving from one cloud to another.

Companies wishing to move on from outdated and increasingly inefficient legacy infrastructures, such as aging servers or potentially unreliable firewall appliances, or to abandon hardware or software solutions that are no longer operating at optimum capacity, are now turning to the cloud to experience the benefits of cloud computing. This is why so many organizations are, at the very least, making a partial migration to the cloud.
We know that cloud migration is critical for achieving real-time and updated performance and efficiency. As such, the process requires careful analysis, planning, and execution to ensure the cloud solution's compatibility with your business requirements.

When considering your strategy for migrating to the cloud, it's important to understand that it's not just about getting there, it's also about what you do when you get there. For instance, what are your options for rebuilding applications so they can perform optimally in the cloud? The process of cloud migration is making companies ask the question: what is application modernization?
There are many questions to be answered along the way, and businesses of all sizes require assistance in making their cloud journeys. Consequently, many services firms can make a strong case for their lift-and-shift cloud migration capabilities, or their classic modernization services, such as automated language translation and conventional re-platforming.

What are the benefits of cloud migration?

For companies that undertake the process of cloud migration, the cloud can have a massive impact.
This includes a reduction in the total cost of ownership (TCO), faster time to delivery, and enhanced opportunities for innovation. With access to the cloud comes agility and flexibility, both of which are imperative to meet changing consumer and market demands.
In recent months, companies have been migrating their services and data to the cloud as they adapt to become elastic digital workplaces to deal with an increase in online demand and remote working. For businesses that have already begun the move to cloud computing, they're accelerating a cloud transformation that will lead the way forward in the years to come.

Benefits of migrating to the cloud include:

- Increased agility and flexibility
- Ability to innovate faster
- Ease of increasing resource demands
- Better management of increased customer expectations
- Reduction in costs
- Deliver immediate business results
- Simplify IT
- Shift to everything-as-a-service
- Better consumption management
- Cloud scalability
- Improved performance

SLA Basics

- Describes a set of non functional requirements of the service.
- Example : RTO time – Return to Operation Time if case of failure

- SLO – Service Level Objective. That is, the objective to be achieved.
- KPI – Key Performance Indicators
- **Service Level Objective:**
- Objective of service quality that has to be achieved.

- Set of measurable KPIs with thresholds to decide if the objective is fulfilled or not.

SLA Basics

- The fulfillment of an SLOs describes a state of service when all of the SLOs key performance indicators are within a specified thresholds.
- KPIs usually consist from one or more raw monitored values including min, avg and max specifying the scale
- They can also represent some aggregated measurement (e.g. average output) within a sliding window that is combined from one or more monitoring outputs.
- The Cloud Computing infrastructures are usually large scale, therefore SLAs need to be formally described to enable their automated handling and protection.

Automated SLA protection

- Automated SLA protection is based on a set of policy rules.
- Each policy rule is formed by one or more conditions (KPI's value matching pattern) and one or more actions.
- KPIs are periodically evaluated according to defined policies.
- If one or more conditions are met, then appropriate actions are triggered.

Important points

- Service Level Agreement (SLA) describes agreement on non-functional requirements between provider and customer.
- SLA consists of service level objectives (SLOs) that are evaluated according to measurable Key Performance Indicators (KPIs).
- Automatic SLA protection enables further increase of the system utilization and system profit.
- In currently available systems only some basic SLAs like "uptime over a time period guarantee" are available.

SLA Requirements

- A signed agreement with each customer.
- Transactions by hour and jobs by day for each application.
- A method of reporting SLA results.
- Priority of services in case of insufficient availability.
- Agreed methods of penalty in case customer exceeds his limits.
- Agreed methods of penalty in case cloud provider fails to meet contract specifications.
- Schedule of virtual or actual meeting between the customer and the cloud provider if necessary.

Compensation within the SLA

For the effective implementation of the SLA, there should be an element that covers the consequences of not meeting the said standards or requirements. The results will have a financial impact and be spelled out in the agreement.

For instance, the agreement provides for reporting services like a financial report with an accuracy of 95%; the contract must state the economic impact for non-adherence to the standard, like for three consecutive failures, a deduction of 10% from the fess or so.

Service Credits

Virtually every cloud application service provider uses service credits as the primary method of compensation under a SLA. A service credit is free use of the cloud service for a certain period of time. Typically, service credits are measured in days of service, such that particular violations of the SLA earn you a certain number of days to use the cloud service free of charge.

When examining a cloud SLA, pay close attention to the definition of a service credit so you can evaluate competing cloud offers side-by-side. If Vendor A defines a service credit as "one day of service" and Vendor B defines a service credit as "1/30th of a monthly subscription charge", you may need to do some quick math to determine the relative dollar values of these credits.

Along with the definition of a service credit, an SLA should explicitly describe the uptime thresholds that entitle you to receive one or more credits. Does a monthly uptime of 99.8% get you one service credit, or three? At what uptime measure do you get additional service credits: 99.5%, 99% or 90%? The SLA should make that clear.

Cloud disaster recovery vs. traditional disaster recovery

Cloud disaster recovery is a cloud computing service which allows for storing and recovering system data on a remote cloud-based platform. To better understand what disaster recovery in cloud computing entails, let's compare it to traditional disaster recovery.

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

Why Choose Disaster Recovery in Cloud Computing

The primary goal of disaster recovery is to minimize the overall impact of a disaster on business performance. Disaster recovery in cloud computing can do just that. In case of disaster, critical workloads can be failed over to a DR site in order to resume business operations. As soon as your production data center gets restored, you can fail back from the cloud and restore your infrastructure and its components to their original state. As a result, business downtime is reduced and service disruption is minimized.

Due to its cost-efficiency, scalability, and reliability, disaster recovery in cloud computing has become the most lucrative option for small and medium-sized businesses (SMBs). Generally, SMBs don't have a sufficient budget or resources to build and maintain their own DR site. Cloud providers offer you access to cloud storage, which can become a cost-effective and long-lasting solution to data protection as well as disaster recovery.

How to Design a Cloud-Based Disaster Recovery Plan

After considering the benefits of cloud computing in disaster recovery, it is time to design a comprehensive DR plan. In fact, you can read one of our blog posts which walks you through **the entire process of a creating a DR plan**. Below, we are going to discuss how to create a DR plan which works in the cloud environment.

As a rule, an effective cloud-based DR plan should include the following steps:

1. Perform a risk assessment and business impact analysis.
2. Choose prevention, preparedness, response, and recovery measures.
3. Test and update your cloud-based DR plan.

Let's discuss how disaster recovery planning works in cloud computing.

The Security Issues and challenges of Cloud Services

Password Security Industrious: password supervision plays a vital role in cloud security. However, the more people you have accessing your cloud account, the less secure it is. Anybody aware of your passwords can access the information you store there. Businesses should employ multi-factor authentication and ensure that passwords are protected and altered regularly, mainly when staff members leave. Access rights related to passwords and usernames should only be allocated to those who require them.

Data privacy: Sensitive and personal information kept in the cloud should be for internal use only, not to be shared with third parties. Businesses must have a plan to securely and efficiently manage the data they gather.

Data Related Security issues

- **Data Breach**: 1.Confidentiality
  2. Integrity
- **Data Lock in**: Users may lose data if they migrate from one vendor to another vendor.
- **Data Remanence:** It is the residual representation of data that have been nominally erased or removed in some way.

Data Related Security issues

- **Data Recovery:** Sometimes server may break down and cause damage or loss to users data. To avoid this, data should be backed up to be recovered in future

- **Data Locality:** In SaaS model of cloud environment, the user doesn't know where the data is stored which may be an issue. The issue can be solved by creating secure SaaS model which can provide reliability to the customer on the location of the data of the user.

Application related security issues

- **Cloud malware injection attack:** In this attack a malicious virtual machine or a service implementation is injected into the cloud system. one solution to prevent this is to perform the integrity check to the service instance.

- **Cookie poisoning:** In this an unauthorized access is made into the application by modifying the contents of the cookie. One solution is to clean up the cookie or encrypt the cookie data.

Application related security issues

- **Backdoor and Debug Option:** Debug option is for the developers who use it to implement any changes requested at later stage in a website since these debug option provides back entry for the developers, sometimes these debug options are left enabled unnoticed, they may provide easy access to the hackers and allow them to make changes in the website.

- **Hidden Field Manipulation**: Certain fields are hidden in the web-site and is used by the developers. Hacker can easily modify on the web page.

- **Guest hopping attack:** An attacker will try get access to one virtual machine by penetrating another virtual machine hosted in the same hardware.

- **SQL injection:** It can be done by injecting the SQL commands into the database of an application to crash the

  database.

CSP level attacks

- **Malicious Insider:** In private cloud, its employee is granted access to the sensitive data of some or all customer administrators. Such privileges may expose information to security threats.

- **Side channel attack:** It occurs when an attacker places a malicious virtual machine on the same physical machine as the victim machine so that he can access all the confidential information on the victims machine.

Network level attacks

- DNS attacks:

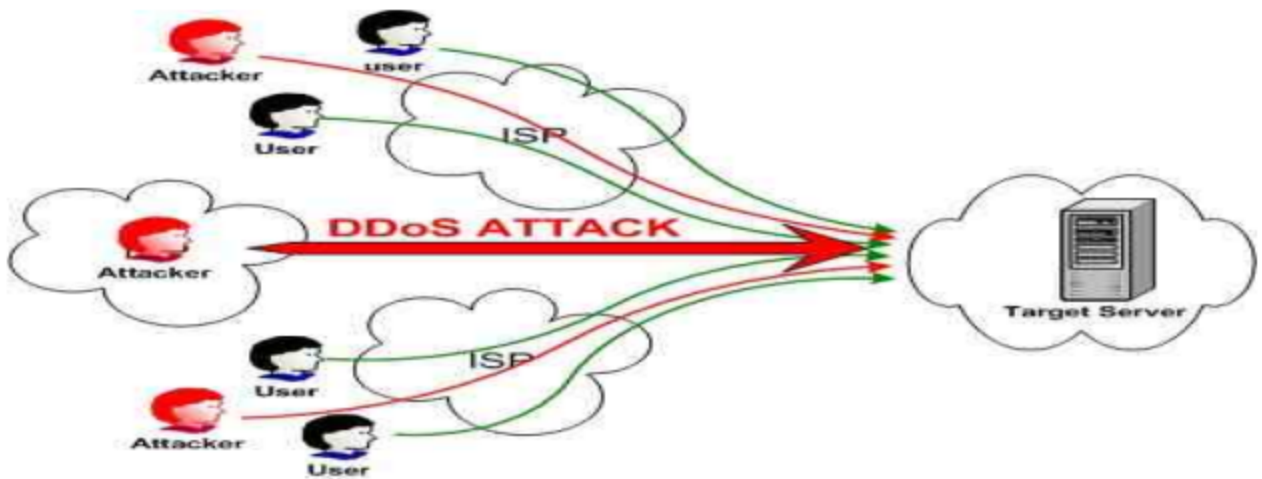
Domain hijacking: Domain hijacking is defined as changing the name of a domain without the knowledge or permission from the domain's owner or creator. This enable the intruders to access the sensitive information.

Cross site scripting: It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials.

Network level attacks

- **IP spoofing:**

  DOS attack: When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests.



Network level attacks

- **Man in the middle attack:** This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured.

- **Network Sniffing:** Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network.