**Cloud computing**[[1]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-urlAn_Introduction_to_Dew_Computing:_Definition''',_Concept_and_Implications_-_IEEE_Journals_&_Magazine-1) is the on-demand availability of [computer](https://en.wikipedia.org/wiki/Computer) [system resources](https://en.wikipedia.org/wiki/System_resource), especially data storage ([cloud storage](https://en.wikipedia.org/wiki/Cloud_storage)) and [computing power](https://en.wikipedia.org/wiki/Computing_power), without direct active management by the user.[[2]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-2) Large clouds often have functions [distributed](https://en.wikipedia.org/wiki/Distributed_computing) over multiple locations, each location being a data center. Cloud computing relies on sharing of resources to achieve coherence[[*clarification needed*](https://en.wikipedia.org/wiki/Wikipedia:Please_clarify)] and [economies of scale](https://en.wikipedia.org/wiki/Economies_of_scale), typically using a "pay-as-you-go" model which can help in reducing [capital expenses](https://en.wikipedia.org/wiki/Capital_expenses) but may also lead to unexpected [operating expenses](https://en.wikipedia.org/wiki/Operating_expense) for unaware users.

 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.

TREACHROUS TWELVE:

**The 12 security threats the CFA identify are:**

* Data breaches
* Insufficient identity, credential and access management
* Insecure interfaces and APIs
* System vulnerabilities
* Account hijacking
* Malicious insiders
* Advanced persistent threats
* Data loss
* Insufficient due diligence
* Abuse and nefarious use of cloud services
* Denial of service
* Shared technology vulnerabilities

### DATA BREACHES

**Threat:** When sensitive data is collected, processed and stored, it can be vulnerable to being intercepted or accessed without permission if the necessary security measures are not in place. Targeted attacks can focus on vulnerabilities in technology and software or utilise other tactics like malware, but data breaches can also simply occur through system misconfigurations or human error.

### 2. INSUFFICIENT IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

**Threat:** The cloud’s accessibility, enabling remote working from anywhere with an internet connection, is one of its (many) selling points. However, if exploited, this potential to connect to networks and platforms from afar can present security risks. Hackers may mask themselves as legitimate users to gain access and use cloud resources and systems.

### INSECURE INTERFACES AND APPLICATION PROGRAMMING INTERFACES (APIS)

**Threat:** Application programming interfaces (APIs) give users the ability to manage, develop and customise their cloud environment. However, this very open and accessible nature can present a cloud security threat, as when individuals and businesses customise cloud services to their needs, there is room for errors and misconfigurations. Interfaces are also typically the most exposed part of a cloud environment, possibly with a public IP address, making it vital they are secure.

### SYSTEM VULNERABILITIES

**Threat:** No software is designed perfectly – there will always be bugs – but the question is whether these bugs present exploitable opportunities for hackers. A cloud operating system is made up of different components, and if one of these has a vulnerability, it presents an opportunity for the system to be infiltrated, affecting the wider cloud environment.

### 5. ACCOUNT HIJACKING

**Threat:** This relates to targeted attempts by individuals to access specific accounts without authorisation, usually ones with high privileges and access to sensitive data. If a cloud account is compromised, it can lead to control of the wider environment. Hackers may aim to steal account credentials through targeting individuals with social engineering techniques such as phishing scams. The victim may then unwittingly hand over their login details.

### 6. MALICIOUS INSIDERS

**Threat:**Not all threats are necessarily located externally. As a trusted individual with access privileges, an insider doesn’t have the problem of passing security defences such as firewalls or authentication controls. If this individual has malicious intentions, they could do immeasurable damage to systems and data integrity.

### 7. ADVANCED PERSISTENT THREATS (ATPS)

**Threat:** An Advanced Persistent Threat (ATP) is a sophisticated cyberattack by a network hacking individual or group. The objectives vary, but the means of attack typically revolve around gaining unauthorised access, compromising systems and stealing data and / or intellectual property – usually inconspicuously, with the aim of remaining undetected and maintaining a presence over a long period of time. Because of this nature, they are often sponsored by a nation or state, or linked to acts of politically motivated cybercrime

### 8. DATA LOSS

**Threat:** Although a data breach can be hugely detrimental to businesses, it’s important to remember data loss can be equally as damaging. Data loss can occur through mistakes and accidents, but also though malicious activity such as ransomware which locks down systems and threatens to delete data if a ransom is not paid. We’re seeing huge increases in ransomware attacks in recent years, with a [365% rise](https://www.csoonline.com/article/3518864/more-targeted-sophisticated-and-costly-why-ransomware-might-be-your-biggest-threat.html) from 2018 to 2019.

### 9. INSUFFICIENT DUE DILIGENCE

**Threat:** It’s important to understand how the cloud effects your functionality and operations, both when it is working and when it isn’t. Although lack of availability should never be allowed to become a persistent problem, there should be a business continuity plan in place for how to remain productive and recover quickly from a period of downtime. Other areas to address when considering a move to the cloud are the commercial, technical, compliance and legal implications for your business.

### 10. ABUSE AND NEFARIOUS USE OF CLOUD SERVICES

**Threat:** Cloud services are widely available and easy to access; any individual or business can purchase and make use of them. However, this presents opportunities for malicious attackers to join the cloud and misuse their access and privileges within that environment whilst posing as a legitimate paying customer. The specific vulnerabilities will depend on the type of cloud service, its infrastructure and overall security, but if cyber criminals successfully register and access cloud services, they can attempt to compromise systems and data of the providers and other users.

### 11. DENIAL OF SERVICE

**Threat:** A Denial of Service (DoS) attack typically overloads resources, either in terms of speed or availability, so that the service is unable to be accessed or used. Common methods include flooding networks with traffic or requests, for example adding huge volumes of items to shopping baskets. Denial of Service attacks come in many forms; one common large-scale variation is a Distributed Denial of Service (DDoS) attack which originates from multiple malicious computers to attack at once from different locations.

### 12. SHARED TECHNOLOGY VULNERABILITIES

**Threat:** This covers the potential security vulnerabilities that can arise from having multiple tenants using different cloud services on the same hardware. If a specific cloud service that one of the tenants is using is compromised, it can open opportunities for attackers to expand that vulnerability to the wider environment and users. This can lead to the loss of data or theft and damage to services or systems.

The six cloud business enablers are applicable whether your cloud strategy involves becoming a consumer or a provider of cloud-based offerings – or includes elements of both Cost flexibility –

1. Shift capex to opex; - IT CapEx is money spent on acquiring physical assets for the purpose of running business. Examples of IT CapEx: printers, servers, laptops, networking equipment, etc. OpEx is money spent on the operational aspect of running business. Examples of IT OpEx: telephone service, leased network lines, printer cartridges. Enterprise software licenses are typically treated as CapEx, along with the servers and networking equipment required to host the software. IT CapEx also tends to be less fluid and much more expensive than routine IT OpEx. CapEx spending also tends to be harder to forecast than OpEx. OpEx typically represents a real cost of doing business: your business needs an internet connection to exist, and you pay for what you use. CapEx in general is often more fuzzy in relation to its impact on a company’s operations, especially when it comes to IT CapEx. Sure, you need a server to run your business, but do you really use it 100% for the entire duration of its life? Even with virtualization tools like VMWare, you’re probably not using it 100%. Plus, CapEx also has maintenance and “unexpected events” overhead that OpEx doesn’t. Cloud enables the shift from CapEx to OpEx.

ii) Pay-per-use software and services; - With cloud applications there is no longer a need to install software or pay software license fees. This pay-per-use model provides greater flexibility and eliminates the need for significant capital expenditures

2) Business Scalability : Businesses can scale operations very easily based on requirement. If you need new servers because the number of hits to your website has increased, then you can easily do so. If you need to get rid of the extra servers, you can do that easily as well

3) Market Adaptability : Cloud enables a faster time to market and helps in rapid prototyping, development and deployment;

4) Masked complexity : The complexity becomes hidden from end-user; There is user independence from IT or other operational issues like upgrade & maintenance.

5) Context-driven variability : Supports user defined preferences. Cloud can be used to store information about user preferences and enable the customization of product or service which is being delivered.

6) Ecosystem connectivity : • Creation of new value nets including SMEs • Shared infrastructure and services from cloud service providers • Enhanced productivity through customer / partner interaction • For example, cloud based platforms support sharing of resources, processes and workforce between companies in Pharmaceutical value chain, hence enabling joint research and collaboration.

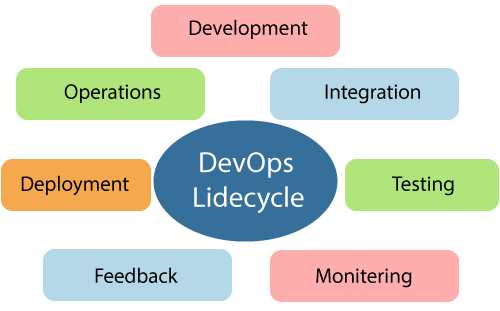
UBER SYNDROME:

Traditional market competition is changing, and the disruption is being driven by what is known as the 'Uber syndrome', whereby a competitor with a completely different business model enters your industry and flattens you. The challenge for CxOs is discovering where the competition will come from and how to respond to it. IBM looked at this phenomenon and others in its C-suite.

**Reconstructing customer-centric processes, predicting the future from the perspective of the ecosystem, and responding to the ongoing future through organizational changes, these three methods are becoming solutions to Uber-style intrusions**

# **DevOps Lifecycle**

DevOps defines an agile relationship between operations and Development. It is a process that is practiced by the development team and operational engineers together from beginning to the final stage of the product.



Learning DevOps is not complete without understanding the DevOps lifecycle phases. The DevOps lifecycle includes seven phases as given below:

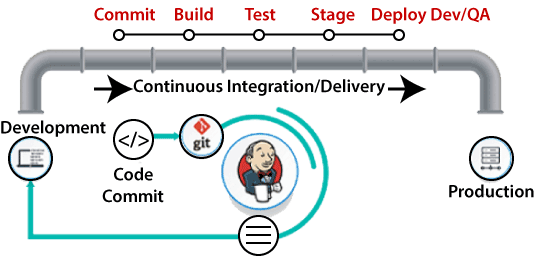
### 1) Continuous Development

This phase involves the planning and coding of the software. The vision of the project is decided during the planning phase. And the developers begin developing the code for the application. There are no DevOps tools that are required for planning, but there are several tools for maintaining the code.

### 2) Continuous Integration

This stage is the heart of the entire DevOps lifecycle. It is a software development practice in which the developers require to commit changes to the source code more frequently. This may be on a daily or weekly basis. Then every commit is built, and this allows early detection of problems if they are present. Building code is not only involved compilation, but it also includes **unit testing, integration testing, code review**, and **packaging**.

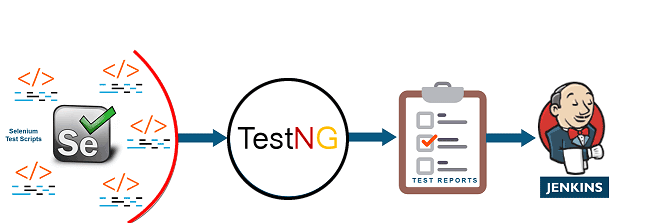
The code supporting new functionality is continuously integrated with the existing code. Therefore, there is continuous development of software. The updated code needs to be integrated continuously and smoothly with the systems to reflect changes to the end-users.



Jenkins is a popular tool used in this phase. Whenever there is a change in the Git repository, then Jenkins fetches the updated code and prepares a build of that code, which is an executable file in the form of war or jar. Then this build is forwarded to the test server or the production server.

### 3) Continuous Testing

This phase, where the developed software is continuously testing for bugs. For constant testing, automation testing tools such as **TestNG, JUnit, Selenium**, etc are used. These tools allow QAs to test multiple code-bases thoroughly in parallel to ensure that there is no flaw in the functionality. In this phase, **Docker** Containers can be used for simulating the test environment.



**Selenium** does the automation testing, and TestNG generates the reports. This entire testing phase can automate with the help of a Continuous Integration tool called **Jenkins**.

Automation testing saves a lot of time and effort for executing the tests instead of doing this manually. Apart from that, report generation is a big plus. The task of evaluating the test cases that failed in a test suite gets simpler. Also, we can schedule the execution of the test cases at predefined times. After testing, the code is continuously integrated with the existing code.

### 4) Continuous Monitoring

Monitoring is a phase that involves all the operational factors of the entire DevOps process, where important information about the use of the software is recorded and carefully processed to find out trends and identify problem areas. Usually, the monitoring is integrated within the operational capabilities of the software application.

It may occur in the form of documentation files or maybe produce large-scale data about the application parameters when it is in a continuous use position. The system errors such as server not reachable, low memory, etc are resolved in this phase. It maintains the security and availability of the service.

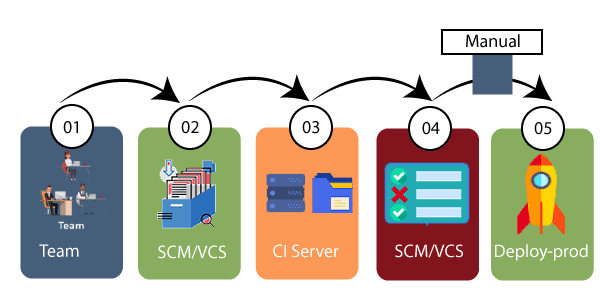
### 5) Continuous Feedback

The application development is consistently improved by analyzing the results from the operations of the software. This is carried out by placing the critical phase of constant feedback between the operations and the development of the next version of the current software application.

The continuity is the essential factor in the DevOps as it removes the unnecessary steps which are required to take a software application from development, using it to find out its issues and then producing a better version. It kills the efficiency that may be possible with the app and reduce the number of interested customers.

### 6) Continuous Deployment

In this phase, the code is deployed to the production servers. Also, it is essential to ensure that the code is correctly used on all the servers.



The new code is deployed continuously, and configuration management tools play an essential role in executing tasks frequently and quickly. Here are some popular tools which are used in this phase, such as **Chef, Puppet, Ansible**, and **SaltStack**.

Containerization tools are also playing an essential role in the deployment phase. **Vagrant** and **Docker** are popular tools that are used for this purpose. These tools help to produce consistency across development, staging, testing, and production environment. They also help in scaling up and scaling down instances softly.

Containerization tools help to maintain consistency across the environments where the application is tested, developed, and deployed. There is no chance of errors or failure in the production environment as they package and replicate the same dependencies and packages used in the testing, development, and staging environment. It makes the application easy to run on different computers.

### 7) Continuous Operations

All DevOps operations are based on the continuity with complete automation of the release process and allow the organization to accelerate the overall time to market continuingly.

It is clear from the discussion that continuity is the critical factor in the DevOps in removing steps that often distract the development, take it longer to detect issues and produce a better version of the product after several months. With DevOps, we can make any software product more efficient and increase the overall count of interested customers in your product.