

IaaS

Used by
swtchitects

It gives access
to the resources
like virtual
machine & storage.

It is popular
among developers
& researchers.

It requires
technical
knowledge.

AWS, vCloud
Express are
cloud services

It is highly
scalable & flexible.

PaaS

Used by
developers

It gives access to
run time environment
to deployment &
devl. tools for app.

It is popular among
developers who focus
on the development
of apps & script.

Some knowledge is
required for the
basic setup.

Facebook & Google
search engine are
cloud services.

It is highly scalable
to suit the different
businesses a/c to
resources.

SaaS

Used by the
end user

It gives access
to the end
user.

It is popular among
consumers & companies
such as file sharing
, email & networking.

There is no requirement
about technicalities
company handles everything.

MS office web &
Google Apps.

It is highly scalable
to suit the small,
mid & enterprise
level business.

(A)

AWS

- Amazon Web Services is a cloud computing platform that offers a range of on-demand operations.
- AWS provides:
Computer power, Content delivery, Database storage, Servers, Storage, Security.
- AWS is a mix of
 - IaaS
 - PaaS
 - SaaS
- AWS is flexible, reliable, scalable & easy to use. It provides access to:
 - Data storage space
 - Networking features

⇒ Here are some key aspects of AWS:-

① Service Offering:-

② Pay-as-You-go Pricing

Here users are billed only for the resources & services they consume.

③ Developer friendly

AWS offers a variety of tools & SDKs for different programming languages making it developer friendly.

② Microsoft Azure

- Also known as Windows Azure.
- It supports various operating systems, databases, programming languages, frameworks that allows IT professionals to easily build, deploy & manage applications through a worldwide n/w.
- It provides scalable, flexible & cost effective.
- It allows developers to quickly manage the applications & websites.
- It offers a Content Delivery System (CDS) for delivering the images, videos, audios & applications.
- 24/7 cooperative team paying attention to their customers.
 - A free trial version of Microsoft Azure is available for 30 days.

③ Google Cloud

- Google cloud platform is a product of Google.
- Google cloud has a firm grip over the banking & finance sector.
- Google Cloud platform is available in 22 regions, 61 zones & 200+ countries.
- GCP offers the cheapest cloud services in the market.
- Easy migration of data without touching any codes.

④ IBM Cloud

- Developed by IBM
- It offers IaaS, SaaS & PaaS services via public, private, hybrid & multi-cloud models.
- Users can manage their application in many coding languages such as Java, Python, PHP, etc.
- Cost depends on usage but free in its lite mode.
- Services offered by IBM cloud are security, database, AI, IoT, Mobile, Private cloud & VMware.

Q. How we provide data privacy & protection in cloud?

① DATA CLASSIFICATION

Begin by categorizing your data based on its sensitivity & importance. Identify which data requires the highest ~~at~~ level of importance / protection & prioritize accordingly.

② ENCRYPTION

Use secure communication protocols to encrypt data as it moves b/w your systems & the cloud.

③ MULTI-FACTOR AUTHENTICATION (MFA)

It requires to add an extra layer of security, making it more difficult for unauthorized individuals to gain access.

④ AUDITING & MONITORING

Enable audit logs & monitoring tools provided by your cloud provider to track access & activities related to your data.

⑤

3rd Party Security

If using 3rd party services or SaaS in the cloud, assess their security practices & ensure they align with your data protection requirements.

⑥

EMPLOYEE TRAINING

Train employees on data security best practices & create awareness about the importance of data protection in the cloud.

* Cloud Security

It refers to the set of measures, practices & technologies designed to protect data, applications & infrastructure in cloud computing environments.

⇒ Benefits

- (a) Protecting ~~from~~ the Business from Dangers.
- (b) Break the Malware & Ransomware attacks.
- (c) Preventing data loss.
- (d) Protecting against internal threats.

Cloud Security

Traditional IT Security

Quick scalable

Slow scaling

Usage based cost

Higher cost

3rd party data centres

In-house data centres.

Efficient resource utilization.

Lower efficiency.

→ Security Challenges in CC

① Data Breaches:

It can occur if unauthorized users gain ~~acces~~ access to sensitive data stored in the cloud.

② Data loss:

It occurs due to h/w failure, s/w bugs or human error.

③ DDoS Attacks:

It can disrupt cloud services by overwhelming them with traffic. Implementing DDoS mitigation strategies is essential to maintain service availability.

④ Enlarged Surface:

Public cloud environments have become a large & highly attractive surface for hackers & disrupt workloads & data in the cloud.

⑤ Data Encryption:

Encrypting data both in transit & at rest is essential to protect sensitive information.

⑥ Vulnerabilities :-

Cloud resources, including virtual machines & containers can be susceptible to security vulnerabilities.

To address these security challenges, organizations should adopt a comprehensive cloud security strategy that includes risk assessment, security policies & regular security audits.

⇒ Threats in CC.

Threats in CC refer to potential risks & security challenges that can compromise the confidentiality, integrity & availability of data & services hosted in cloud environments.

① Data Breaches

② DDoS Attacks

③ IAM (Inadequate Identity & Access Management)

Poorly managed user identities & access controls can result in unauthorized access to cloud resources.

④ Phishing Attacks

Targeting cloud users can lead to stolen credentials & unauthorized access to cloud accounts & data.

⑤ Lack of Visibility & Control :-

Organizations may have limited visibility & control over the security of cloud resources, in IaaS & PaaS models.

Q. Explain compliance & legal issues in the cloud.

Compliance & legal issues in the cloud are critical considerations for organizations using cloud services to store, process or manage data.

Some of key compliance & legal issues in the cloud computing are:

① Industry-Specific Regulations

Various industries & govt. have their own regulatory frameworks governing data security & privacy. Cloud users in these sectors must ensure their cloud providers offer compliant services.

② Security Standards

Many compliance provide security guidelines & best practices for securing cloud environments. Organizations may need to adhere to meet requirements

③ Vendor Compliance

Organizations must verify that their chosen cloud provider complies with relevant regulations & industry standards.

IAM

- Identity Access Management is a fundamental component of cloud computing.
- IAM is crucial for ensuring the security, privacy & compliance of cloud based systems & data.
- It helps organizations strike a balance b/w enabling users to access the resources they need and safeguarding against unauthorized access & data breaches.