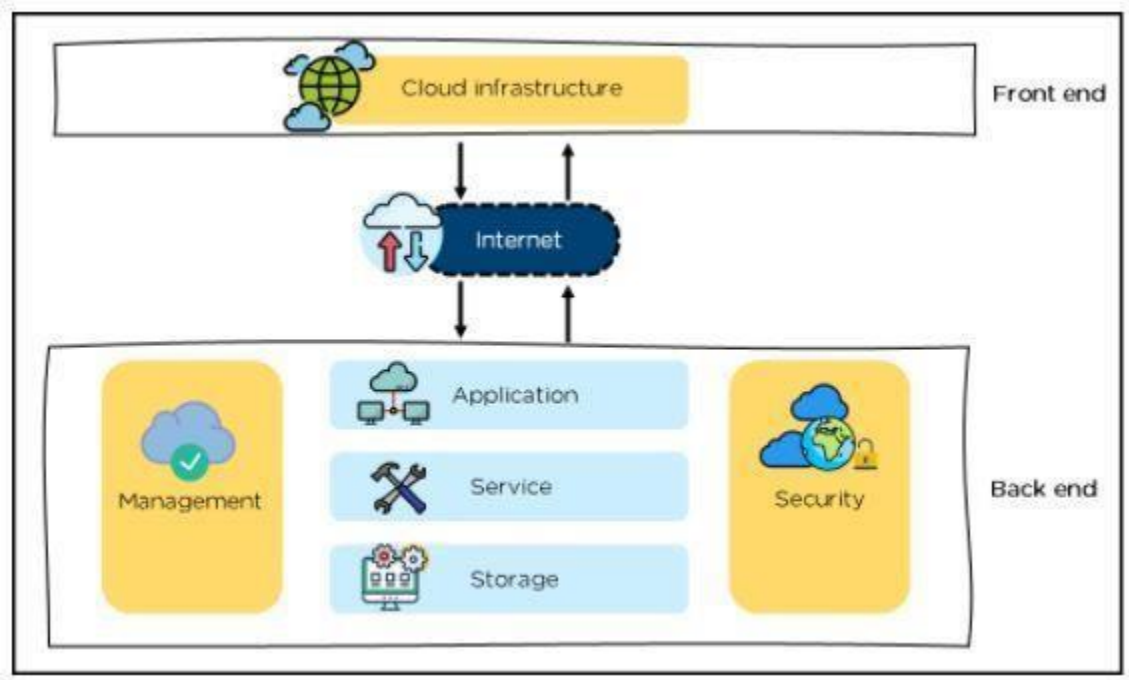
Cloud computing architecture

Cloud computing architecture refers to the structure and components that enable cloud services. Cloud Computing Architecture is divided into two parts:

- front-end
- back-end

Front-end and back-end communicate via a network or internet.



Front-End

- Provides applications and the interfaces required for the cloud-based service.
- Consists of client's side applications (web browsers) such as Google Chrome and Internet Explorer.
- Cloud infrastructure is the only component of the front-end and consists of Computers, smartphones, or IoT devices that access the cloud.

- Provides a Graphical User Interface to the end-users to perform respective tasks

Back-End

Responsible for monitoring all the programs that run the application on the front end. It has a large number of data storage systems and servers.

The components of the back end cloud architecture are mentioned below.

- Application**:** Software or a platform which provides the result to the end- user (with resources).
- Service**:** Provide utility in the architecture, widely used services are storage application development environments and web services
-
- Storage**:** It stores and maintains data like files, videos, documents, etc. over the internet. Eg: Amazon S3, Oracle Cloud-Storage, Microsoft Azure Storage
- Management: Its task is to allot specific resources to a specific task and establishes coordination among the cloud resources. It helps in the management of components like application, task, service, security, data storage, and cloud infrastructure.
- Security: Implements security management to the cloud server with virtual firewalls. It provides secure cloud resources, systems, files, and infrastructure to end-users

Components of Cloud Computing architecture

Hypervisor

- It is also called Virtual Machine Monitor (VMM).
- It is software, firmware, or hardware that creates and manages virtual machines (VMs) by allowing multiple operating systems to run on a single physical machine.
- It is a virtual machine monitor which provides Virtual Operating Platforms to every user
- Manages guest operating systems in the cloud
- It runs a separate virtual machine on the back end which consists of software and hardware
- Its main objective is to divide and allocate resources

Management Software

- Its responsibility is to manage and monitor cloud operations with various strategies to increase the performance of the cloud
- Some of the operations performed by the management software are: compliance, auditing management of overseeing disaster contingency plans.

Deployment Software

- It consists of all the mandatory installations and configurations required to run a cloud service
- All deployment of cloud services is performed using a deployment software
- The three different models which can be deployed are: SaaS, PaaS, IaaS

Network

- It connects the front-end and back-end.
- Allows every user to access cloud resources
- Helps users to connect and customize the route and protocol

Cloud Server

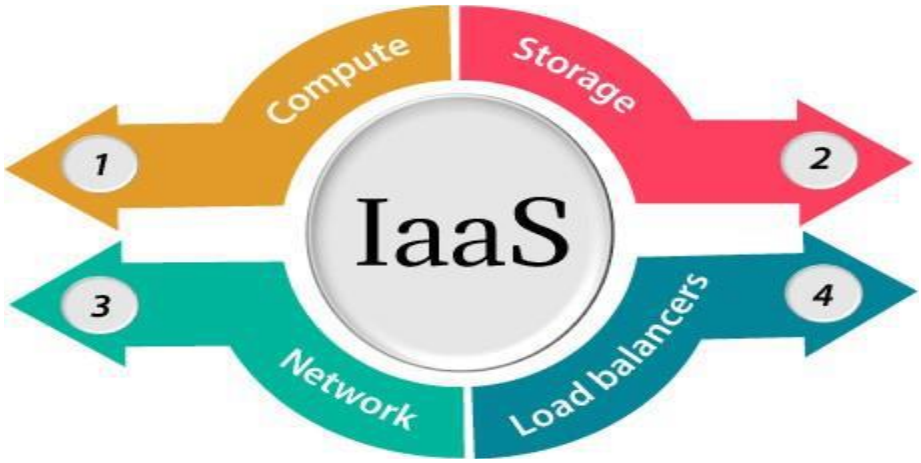
- It is a virtual server which is hosted on the cloud computing platform
- It is highly flexible, secure, and cost-effective

Cloud Storage

- Here, every bit of data is stored and accessed by a user from anywhere over the internet
- It is scalable at run-time and is automatically accessed
- Data can be modified and retrieved from cloud storage over the web

Infrastructure as service(IaaS)

- Infrastructure as a Service (IaaS) is one of the three fundamental service models of cloud computing alongside Platform as a Service (PaaS) and Software as a Service (SaaS).
- Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components.
- The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.
- Clients are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment.
- API access to the infrastructure may also be offered as an option.
- Some examples of service provider are Amazon Web Services (AWS), Google Compute Engine (GCE), Openstack.
- IaaS provider provides the following services –



- Compute: Computing as a Service includes virtual central processing units and virtual main memory for the VMs that is provisioned to the end- users.

- Storage: IaaS provider provides back-end storage for storing files.
- Network: Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the VMs.

- Load balancers: It provides load balancing capability at the infrastructure layer.

Key features of IaaS

- Instead of purchasing hardware completely, users pay for IaaS on demand.
- Infrastructure is scalable depending on processing and storage needs.
- Saves enterprises the costs of buying and maintaining their hardware.
- Because data is on the cloud, there can be no single point of failure.
- Enables the virtualization of administrative tasks, freeing up time for other work.

Advantages of IaaS Cloud Computing

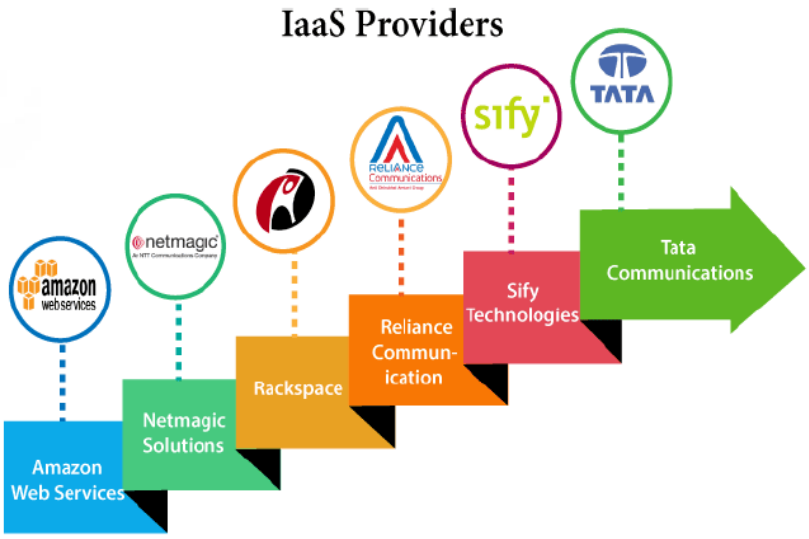
- Shared Infrastructure - Allows multiple users to share the same physical infrastructure.
- Web access to the Resources - Allows IT users to access resources over the internet.

- Pay-as-per-use Model - IaaS providers provide services based on the pay-as-per-use basis.
- Focus on the Core Business - IaaS providers focus on the organization's core business rather than on IT infrastructure.
- On-demand Scalability - Users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Disadvantages of IaaS Cloud Computing

- Layer Security - Most of the IaaS providers are not able to provide 100% security.
- Interoperability issues - It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

Top IaaS Providers who are providing IaaS Cloud Computing platform



Amazon Elastic Compute Cloud (EC2) is a web service that provides scalable computing capacity in the cloud. (signup AWS account and test for Iaas)

Platform as a Service (PaaS)

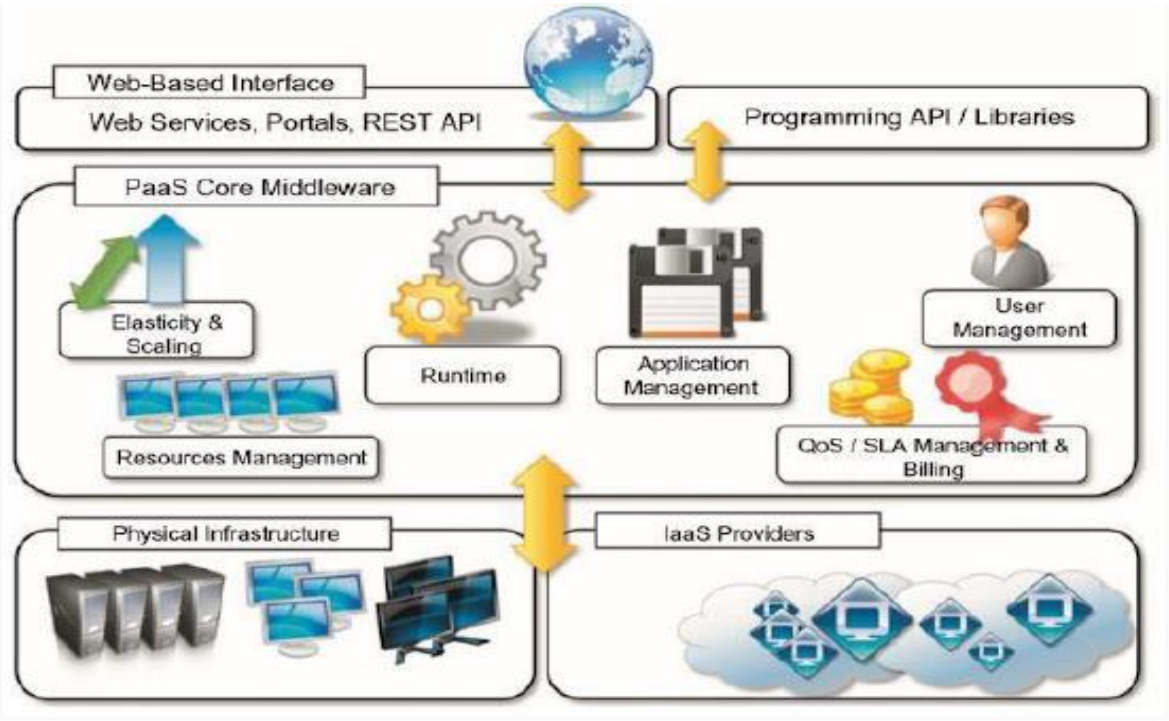
Provides a computing platform with a programming language execution environment and a development and deployment platform for running applications in the cloud.

- It constitutes the middleware on top of which applications are built.
- Application management is the core functionality of the middleware.
- Provides run time environments for the applications.

•PaaS provides

- Applications deployment
- Configuring application components
- Provisioning and configuring supporting technologies

- For user, PaaS interfaces can be in the form of a Web-based interface or in the form of programming APIs and libraries.
- PaaS solutions generally include the infrastructure as well.
- Pure PaaS offered only the user-level middleware.
- Some examples: Google App Engine, Azure, AWS, Force.com



PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:

- Programming languages - PaaS providers provide various programming languages for the developers to develop the applications. Eg. Java, PHP, Ruby, Perl, and Go.
- Application frameworks - PaaS providers provide application frameworks to easily understand the application development. Eg. Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.
- Databases - PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.
- Other tools - PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

Characteristics of PaaS:

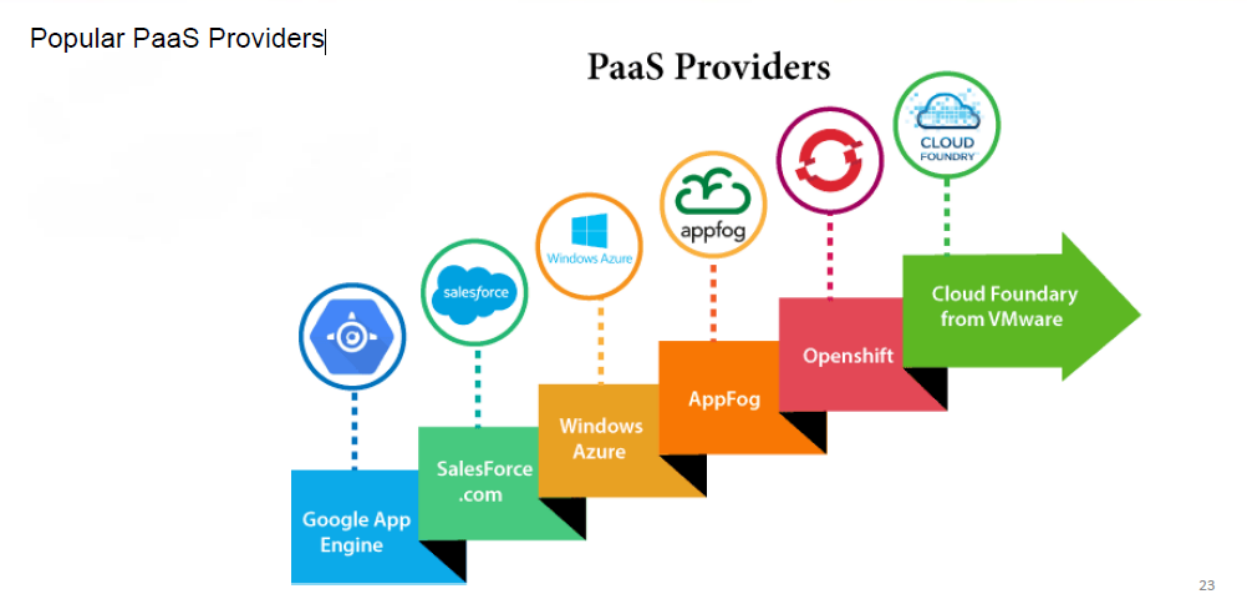
- Runtime framework: The runtime framework executes end-user code according to the policies set by the user and the provider.
- Abstraction: PaaS offer a way to deploy and manage applications on the cloud rather than a virtual machine on top of which the IT infrastructure is built and configured.
- Automation: PaaS deploy the applications automatically.
- Cloud services: Provide services for creation, delivery, monitoring management, reporting of applications

Advantages of PaaS Cloud Computing

- Simplified Development - Allows developers to focus on development and innovation without worrying about infrastructure management.
- Lower risk - No need for up-front investment in hardware and software.
- Prebuilt business functionality - Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.
- Instant community - Provide online communities where the developer can get the ideas to share experiences and seek advice from others.
- Scalability - Applications deployed can scale without any changes to the applications.

Disadvantages of PaaS Cloud Computing

- Vendor lock-in - The migration of an application to another PaaS vendor can become a problem.
- Data Privacy - Corporate data can be a risk in terms of privacy of data.
- Integration with the rest of the systems applications - There will be chances of increased complexity when we want to use data which in the cloud with the locally stored data.



Software as a Service (SaaS)

- Allows users to connect and use cloud-based apps over the Internet.
- SaaS is the service with which end users interact directly.
- It provides a means to free users from complex hardware and software management.
- Do not need to purchase the software and required the license.
- They simply access the application website or use application with their credentials and billing details
- Customer can customize their software.
- Application is available to the customer on demand.
- It can be considered as a "one-to-many" software delivery model.
- Applications are built as per the user needs.

- Some examples: G Suite, Office 365, Dropbox, WhatsApp

Services Provided by SaaS providers

- Business Services -. The SaaS business services include ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), billing, and sales.
- Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents. Example: Slack, Samepage, Box, and Zoho Forms.
- Social Networks - Social networking service providers use SaaS for their convenience and handle the general public's information.
- Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS

Advantages of SaaS Cloud Computing

- SaaS is easy to buy - SaaS pricing is based on a monthly fee or annual fee subscription,
- One to Many - SaaS services are offered as a one-to-many model means a single instance of the application is shared by multiple users.
- Less hardware required for SaaS - Organizations do not need to invest in additional hardware.
- Low maintenance required for SaaS - Software as a service removes the need for installation, set-up, and daily maintenance for the organizations.
- No special software or hardware versions required - All users will have the same version of the software and typically access it through the web browser and reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.
- Multidevice support - Can be accessed from any device such as desktops, laptops, tablets, phones.
- API Integration - SaaS services easily integrate with other software or services through standard APIs.
- No client-side installation - SaaS services are accessed directly from the service provider using the internet connection, so do not need to require any software installation.

Disadvantages of SaaS Cloud Computing

- Security – Since data is stored in the cloud it is not as secure as in-house deployment.

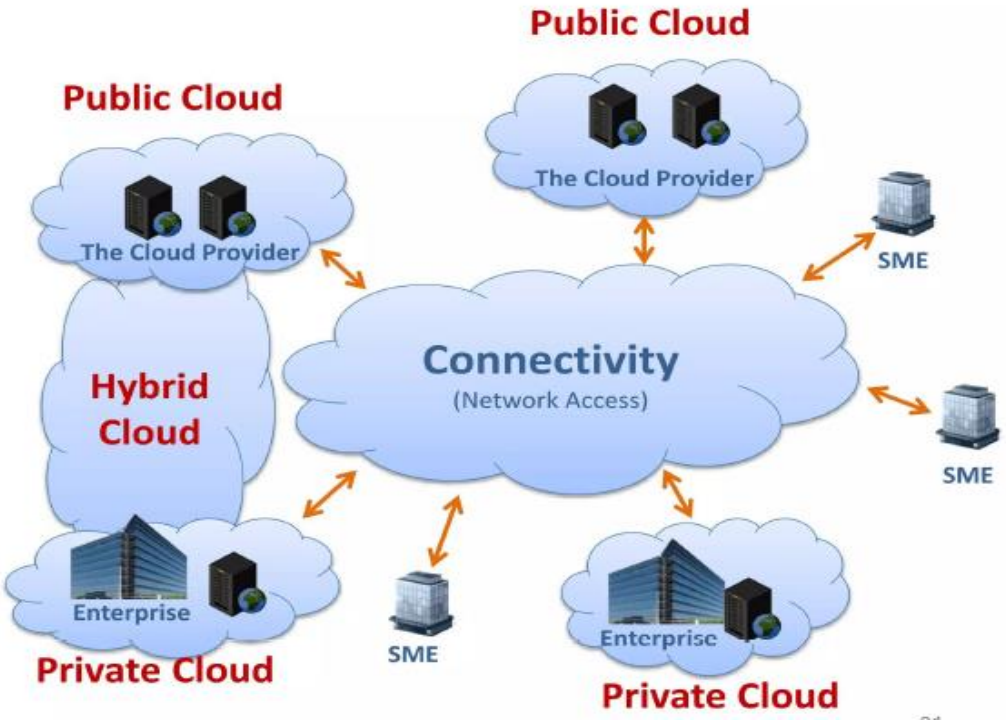
- Latency issue - There may be greater latency when interacting with the application compared to local deployment.
- Total Dependency on Internet - Without an internet connection, most SaaS applications are not usable.
- Switching between SaaS vendors is difficult - Switching SaaS vendors involves the difficult and slow task of transferring the very large data files over the internet and then converting and importing them into another SaaS.

Popular SaaS Providers

Deployment Models

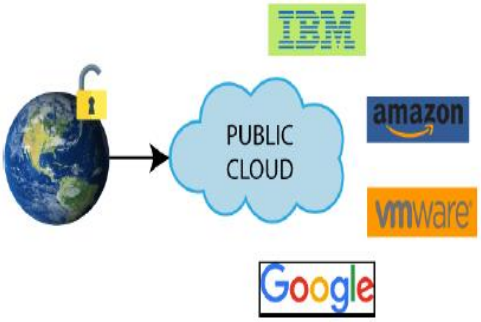
Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access:

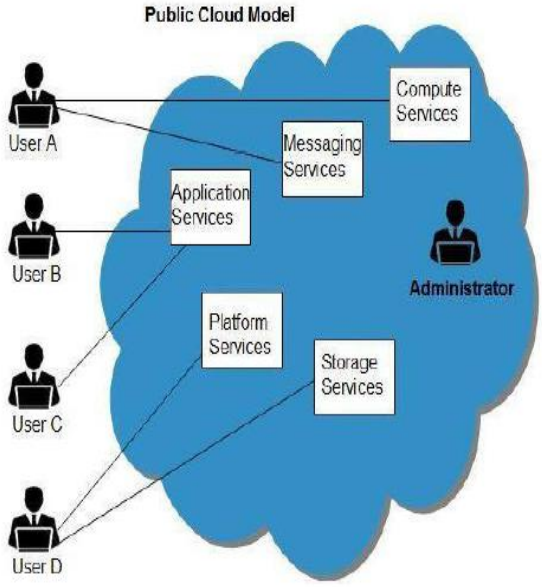
- Public
- Private
- Hybrid
- Community



Public Cloud

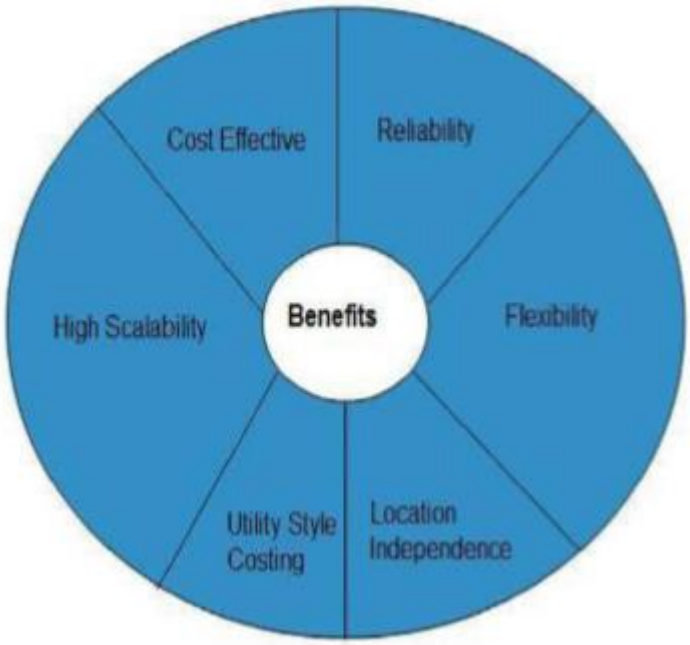
- A public cloud (also called External Cloud) is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet.
- Public cloud services may be free or offered on a pay-per-usage model.
- A public cloud is hosted, operated, and managed by a third-party vendor from one or more data centers.
- In a public cloud, security management and day-to-day operations are referred to the third party vendor, who is responsible for the public cloud service offering.
- Hence, the customer of the public cloud service offering has a low degree of control and an oversight of the physical and logical security aspects of a private cloud.





Advantages

There are many benefits of deploying cloud as public cloud model. The following diagram shows some of those benefits:



- Cost Effective: Since public cloud shares same resources with large number of customers it turns out inexpensive.
- Reliability: The public cloud employs large number of resources from different locations. If any of the resources fails, public cloud can employ another one.
- Flexibility: The public cloud can smoothly integrate with private cloud, which gives customers a flexible approach.
- Location Independence: Public cloud services are delivered through Internet, ensuring location independence.

- Utility Style Costing: Public cloud is also based on pay-per-use model and resources are accessible whenever customer needs them.
- High Scalability: Cloud resources are made available on demand from a pool of resources, i.e., they can be scaled up or down according the requirement.

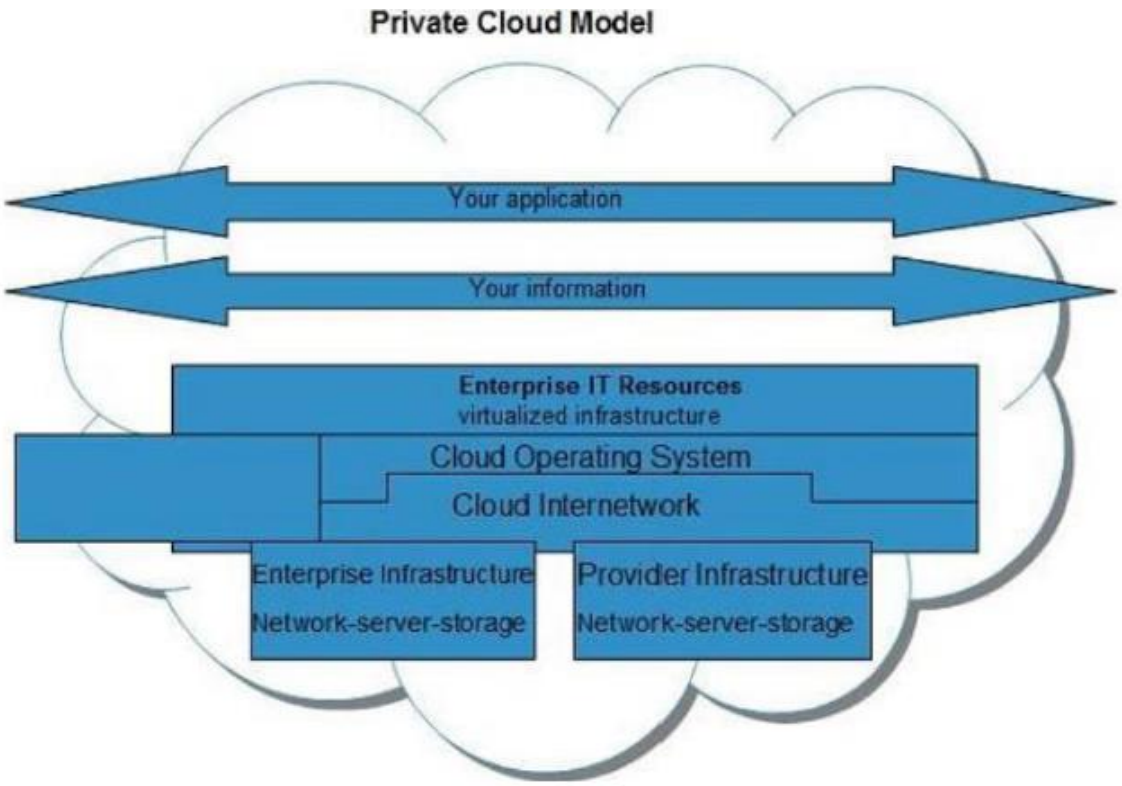
Disadvantages

Here are some disadvantages of public cloud model:

- Low Security: In public cloud model, data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.
- Less Customizable: It is comparatively less customizable than private cloud.

Private Cloud

- A Private Cloud is a cloud computing environment dedicated to a single organization.
- Private Cloud allows systems and services to be accessible within an organization. The Private Cloud is operated only within a single organization.
- However, it may be managed internally by the organization itself or by third-party.
- Private Cloud Deployment Models can be
    - On-Premises Private Cloud – Hosted within the organization's data center.
    - Managed Private Cloud – Hosted by a third-party provider but dedicated to a single organization.
    - Virtual Private Cloud (VPC) – A private section within a public cloud with isolated resources.



Private Cloud provider**:** VMware, OpenStack, Azure Stack

Advantages

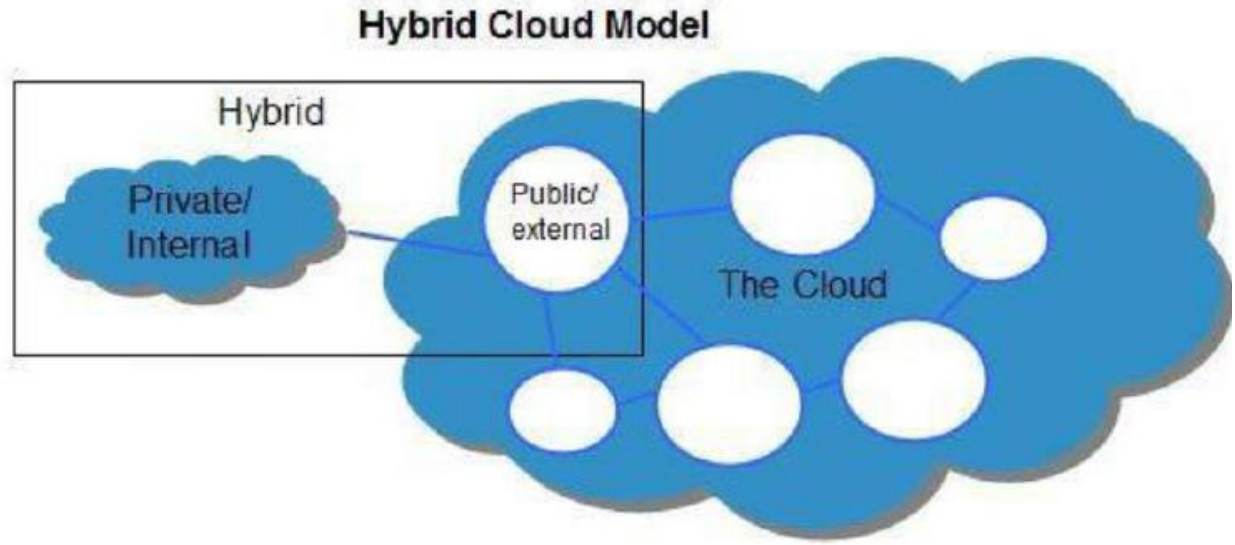
- Higher security and privacy - Private cloud operations are not available to general public and resources are shared from distinct pool of resources, therefore, ensures high security and privacy.
- More control - Private clouds have more control on its resources and hardware because it is accessed only within an organization.
- Cost and energy efficiency - Private cloud resources are not as cost effective but they offer more efficiency than public cloud.
- Improved Reliability

Disadvantages

- Restricted area - Only accessible locally and is difficult to deploy globally.
- Inflexible pricing – To meet demand, purchasing new hardware is very costly.
- Limited scalability - Can be scaled only within capacity of internal hosted resources.
- Additional skills - In order to maintain cloud deployment, organization requires more skilled and expertise

Hybrid Cloud

Hybrid Cloud is a mixture of public and private cloud. Non-critical activities are performed using public cloud while the critical activities are performed using private cloud. The Hybrid Cloud Model is shown in the diagram below.



Advantages

- Scalability - It offers both features of public cloud scalability and private cloud scalability.
- Flexibility - It offers both secure resources and scalable public resources.
- Cost efficiencies - Public cloud are more cost effective than private, therefore hybrid cloud can have this saving.
- Security - Private cloud in hybrid cloud ensures higher degree of security.

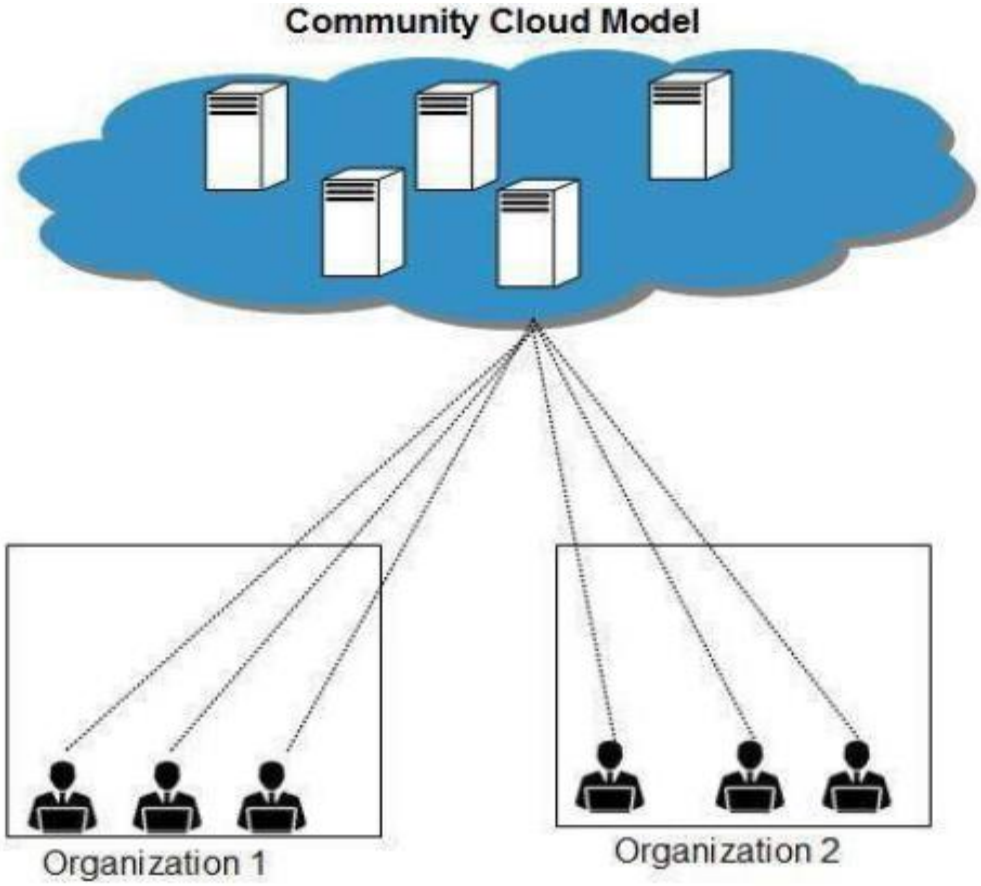
Disadvantages

- Networking issues - Networking becomes complex due to presence of private and public cloud.
- Security compliance - It is necessary to ensure that cloud services are compliant with organization's security policies.
- Infrastructural dependency - The hybrid cloud model is dependent on internal IT infrastructure; therefore, it is necessary to ensure redundancy across data centers.

Community Cloud

Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a

specific community. It may be managed internally by organizations or by the third-party. The Community Cloud Model is shown in the diagram below.



Advantages

- Cost effective – It offers same advantage as that of public cloud at low cost. Sharing between organizations community cloud provides an infrastructure to share cloud resources and capabilities among several organizations.
- Security - It is comparatively more secure than the public cloud.

Disadvantages

- Since all data is housed at one location, it might be accessible by others.
- It is also challenging to allocate responsibilities of governance, security and cost.

THE COMPARATIVE ANALYSIS OF THE BEST CLOUD DEPLOYMENT MODELS

Parameters	Public	Private	Community	Hybrid
Ease of setup & use	Easy	Requires IT proficiency	Requires IT proficiency	Requires IT proficiency
Data security and privacy	Low	High	Comparatively high	High
Data control	Little to none	High	Comparatively high	Comparatively high
Reliability	Vulnerable	High	Comparatively high	High
Scalability and flexibility	High	High	Fixed capacity	High
Cost-effectiveness	The cheapest one	Cost-intensive, the most expensive one	Cost is shared among community members	Cheaper than a private model but more costly than a public one
Demand for in-house hardware	No	Depends	Depends	Depends

Choosing the Right Cloud Model

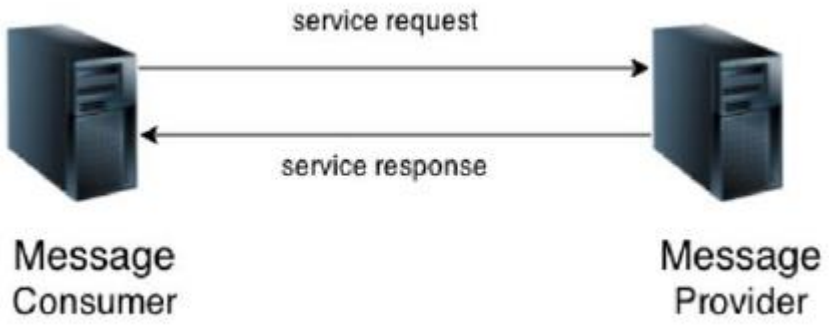
When selecting a cloud computing model**,** organizations must consider cost, security, scalability, compliance and business needs**.**

- If cost and scalability are priorities → Public Cloud
- If security, control, and compliance matter → Private Cloud
- If you need both flexibility and control → Hybrid Cloud

Cloud design and implementation using SOA

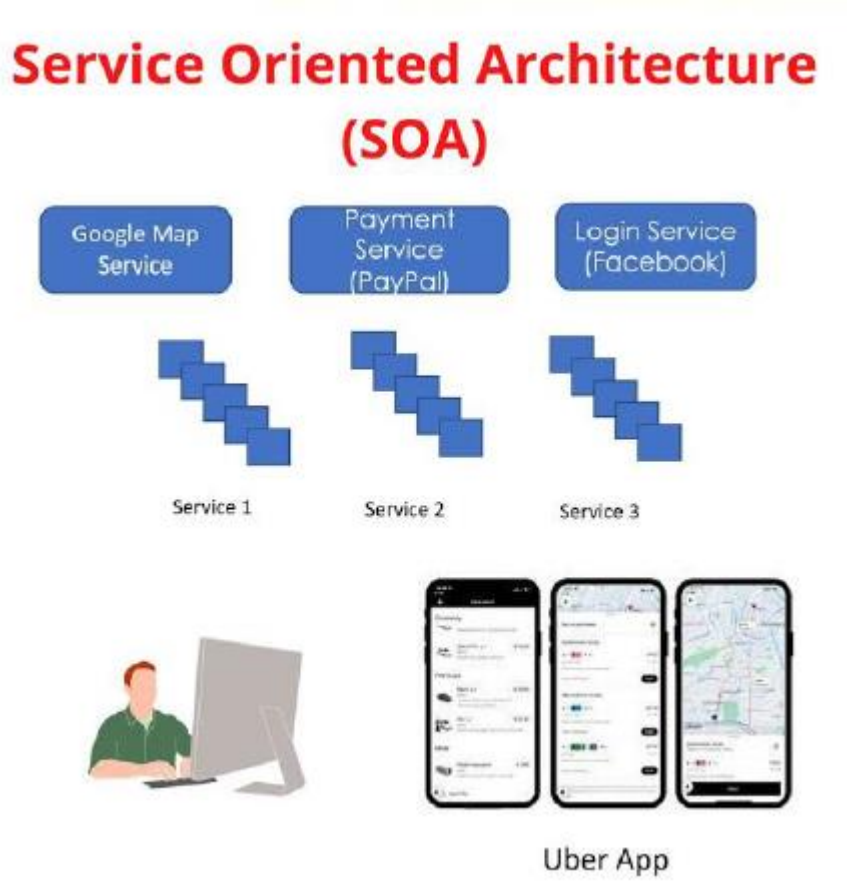
Service

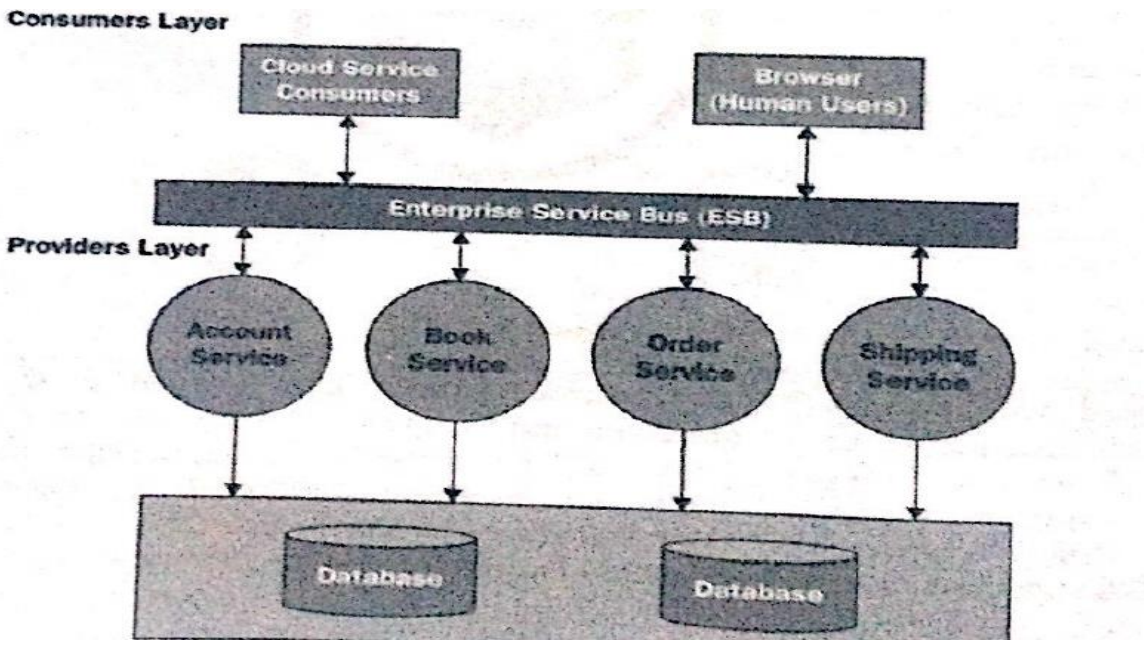
- A service is a well-defined, self-contained function that represents a unit of functionality.
- A service can exchange information from another service.
- It is not dependent on the state of another service.
- It uses a loosely coupled, message-based communication model to communicate with applications and other services.
- Service consumer sends a service request to the service provider, and the service provider sends the service response to the service consumer.
- The service connection is understandable to both the service consumer and service provider.



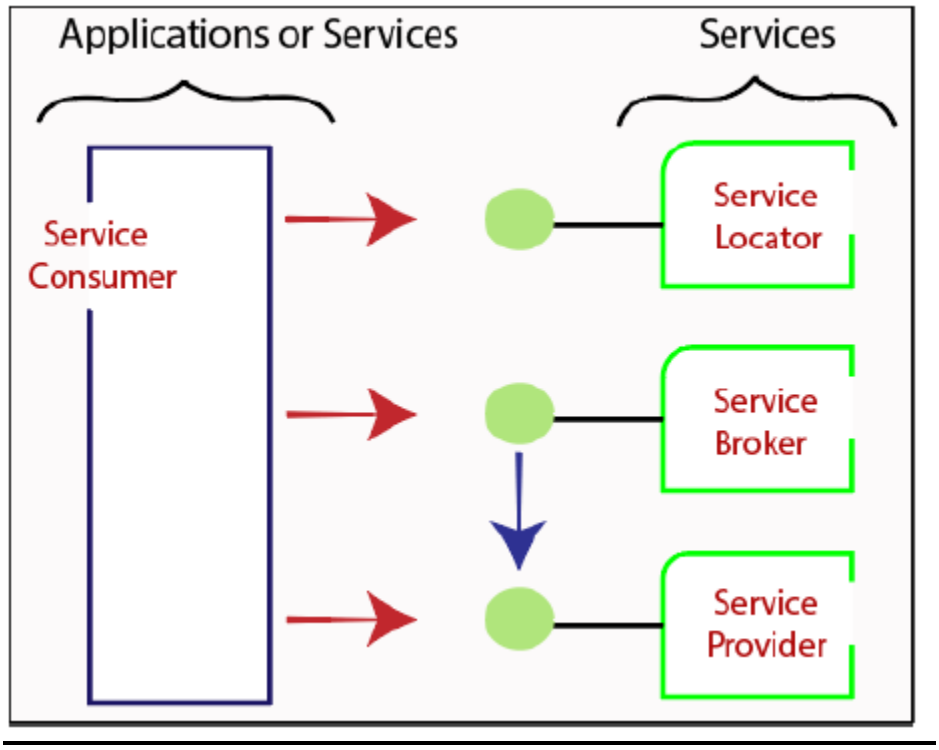
Service Oriented Architecture (SOA)

- Service-Oriented Architecture (SOA) is a software design approach that involves building software components as reusable services.
- Each service represents a specific business function and can be accessed over a network using standard protocols.
- In cloud design and implementation, SOA is used to create a flexible, scalable, and modular architecture that can support a wide range of applications and services.
- SOA enables the creation of loosely-coupled services that can be combined and orchestrated to support complex business processes.
- SOA is particularly well-suited for cloud computing because it allows for the creation of services that can be accessed from anywhere on the internet.
- This means that applications can be built using services from multiple sources, including public cloud providers, private cloud infrastructure, and legacy systems.
- SOA supports loose coupling everywhere in the project.
- SOA supports interoperability.
- SOA increases the quality of service.
- SOA supports vendor diversity.
- SOA is location-transparent.


Service Oriented Architecture
(SOA)
Google Map Service
Payment Service (PayPal)
Login Service (Facebook)
Service 1
Service 2
Service 3
Uber App


Consumers Layer
Cloud Service Consumers
Browser (Human Users)
Enterprise Service Bus (ESB)
Providers Layer
Account Service
Book Service
Order Service
Shipping Service
Database
Database

Service-Oriented Terminologies

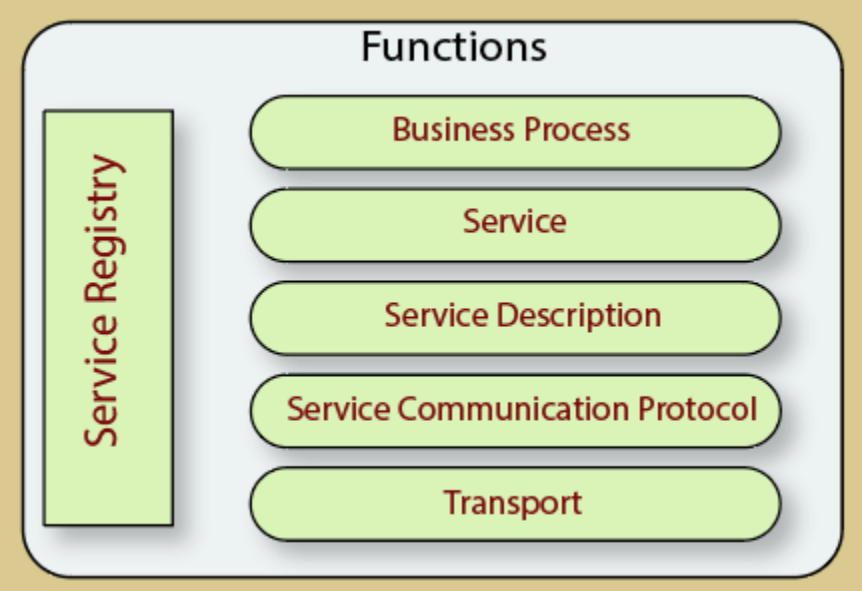


- Services - The logical entities defined by one or more published interfaces.
- Service provider - Software entity that implements a service specification.
- Service consumer - Requestor or client that calls a service provider. A service consumer can be another service or an end-user application.
- Service locator - A service provider that acts as a registry and is responsible for examining service provider interfaces and service locations.
- Service broker - A service provider that pass service requests to one or more additional service providers.

Components of SOA

We discuss the components of SOA with functional aspects and quality of service aspect.

Functional Aspect



Functional Aspects

Transport	It delivers service requests from service consumers to service providers and service responses from service providers to service consumers.
Service Communication Protocol	It enables the communication between the service provider and the service customer.
Service Description	It defines the service and the data needed to use it.
Service	It is a real service.
Business Process	It represents a set of services called in a certain order and connected with specific rules to satisfy the business needs.
Service Registry	It provides information on the data that service providers use to publish their services.

Quality of Service Aspect

Quality of Service (QoS) aspects

Policy	It is the collection of protocols that a service provider uses to create and provide services to customers.
Security	It is the collection of procedures necessary for identification and permission.
Transaction	It ensures that the results are consistent. This indicates that if we utilize the set of services to fulfill a business function, we must finish all of them or none of them.
Management	It specifies the collection of attributes that will be used to administer the services.

Advantages of SOA

- Easy to integrate - The integration is a service specification that provides implementation transparency.
- Manage Complexity - Due to service specification, the complexities get isolated, and integration becomes more manageable.
- Platform Independence - The services are platform-independent as they can communicate with other applications through a common language.
- Loose coupling - It facilitates to implement services without impacting other applications or services.
- Parallel Development - As SOA follows layer-based architecture, it provides parallel development.
- Available - The SOA services are easily available to any requester.
- Reliable - As services are small in size, it is easier to test and debug them.

Disadvantages

- Implementation of SOA requires a large initial investment.
- Service management is complicated since the services exchange millions of messages that are hard to track.

SOA and Cloud

Service-Oriented Architecture (SOA) and Cloud Computing are two architectural approaches that complement each other and can be used together to create flexible, scalable, and interoperable IT systems. SOA provides a framework for organizing and designing software services that can be accessed over a network. When combined with cloud computing, it allows enterprises to create cloud native services that can be accessed, scaled, and managed on-demand.

Monitoring-as-a-Service (MaaS)

Monitoring as a service (MaaS) is one of many cloud delivery models under anything as a service (XaaS). It is a framework that facilitates the deployment of monitoring functionalities for various other services and applications within the cloud. The most common application for MaaS is online state monitoring, which continuously tracks certain states of applications, networks, systems, instances or any element that may be deployable within the cloud.

MaaS offerings consist of multiple tools and applications meant to monitor a certain aspect of an application, server, system or any other IT component. There is a need for proper data collection, especially of the performance and real-time statistics of IT components, in order to make proper and informed management possible.

The tools being offered by MaaS providers may vary in some ways, but there are very basic monitoring schemes that have become ad hoc standards simply because of their benefits. State monitoring is one of them, and has become the most widely

used feature. It is the overall monitoring of a component in relation to a set metric or standard. In state monitoring, a certain aspect of a component is constantly evaluated, and results are usually displayed in real time or periodically updated as a report. For example, the overall timeout requests measured in a period of time might be evaluated to see if this deviates from what's considered an acceptable value. Administrators can later take action to rectify faults or even respond in real time. State monitoring is very powerful because notifications now come in almost every form, from emails and text messages to various social media alerts like a tweet or a status update on Facebook.

Security, Trust and Privacy

- Privacy is about how information is used and shared.
- Security involves protecting systems, assets, and information from unauthorized access or attacks
- Security, Trust and Privacy refers to the critical concept of ensuring that data stored and processed on a cloud platform is protected from unauthorized access, treated with confidentiality and managed in a way that respects user privacy, requiring a high level of trust in the cloud service provider to handle sensitive information responsibly.

Cloud security threats:

- Data breaches: The most significant threat, where unauthorized parties access, steal, or expose sensitive data stored in the cloud, often due to weak access controls or system vulnerabilities.
- Misconfigurations: Errors in setting up or managing cloud services, leaving systems vulnerable to attacks and making it difficult to detect malicious activity.
- Account hijacking: Cybercriminals gaining unauthorized access to user accounts to access sensitive data or launch further attacks.
- Denial of service (DOS: attacks: Attempts to overwhelm a cloud system with traffic, causing service disruptions and hindering user access.
- Insider threats: Malicious actions by employees or privileged users with access to cloud systems, potentially leading to data leaks or unauthorized modifications.
- Insecure APIs: Weak security measures within application programming interfaces (APIs) can expose sensitive data and allow attackers to exploit vulnerabilities.
- Lack of visibility and control: Difficulty in monitoring and managing cloud environments, making it harder to identify potential threats.
- Shared infrastructure vulnerability: When a security flaw in the shared cloud infrastructure can affect multiple users and their data.
- Lack of Awareness

Some security and privacy measures

- Data Encryption: Encrypting data both at rest and in transit to scramble sensitive information and prevent unauthorized access even if intercepted.
- Access Controls: Implementing strict user authentication and authorization mechanisms to Determines who can access what based on policies and permissions within the cloud environment.
- Identity Management: Managing user identities and credentials centrally to ensure proper access control and prevent unauthorized logins.
- Data Governance: Establishing clear policies and procedures for data collection, usage, retention, and disposal to comply with privacy regulations.
- Auditing and Monitoring: Regularly monitoring cloud activity to detect suspicious behavior and potential security breaches.
- Physical Security: Protecting the physical infrastructure where cloud data is stored, including data centers, from unauthorized access.
- Compliance with Regulations: Adhering to relevant data privacy laws.
- Customer Education: Providing users with information and resources to understand cloud security best practices and their own responsibility in data protection

Assignments

- Differentiate public cloud from private cloud.
- What is cloud computing? Describe cloud service models?
- Explain the role of SOA while developing cloud applications.