Lecture Contents

- What is Cloud Computing?
- Early models of Cloud Computing.
- Delivery models and services.
- Ethical issues in Cloud Computing.
- Cloud vulnerabilities.
- Parallel Computing.
- Distributed Systems.

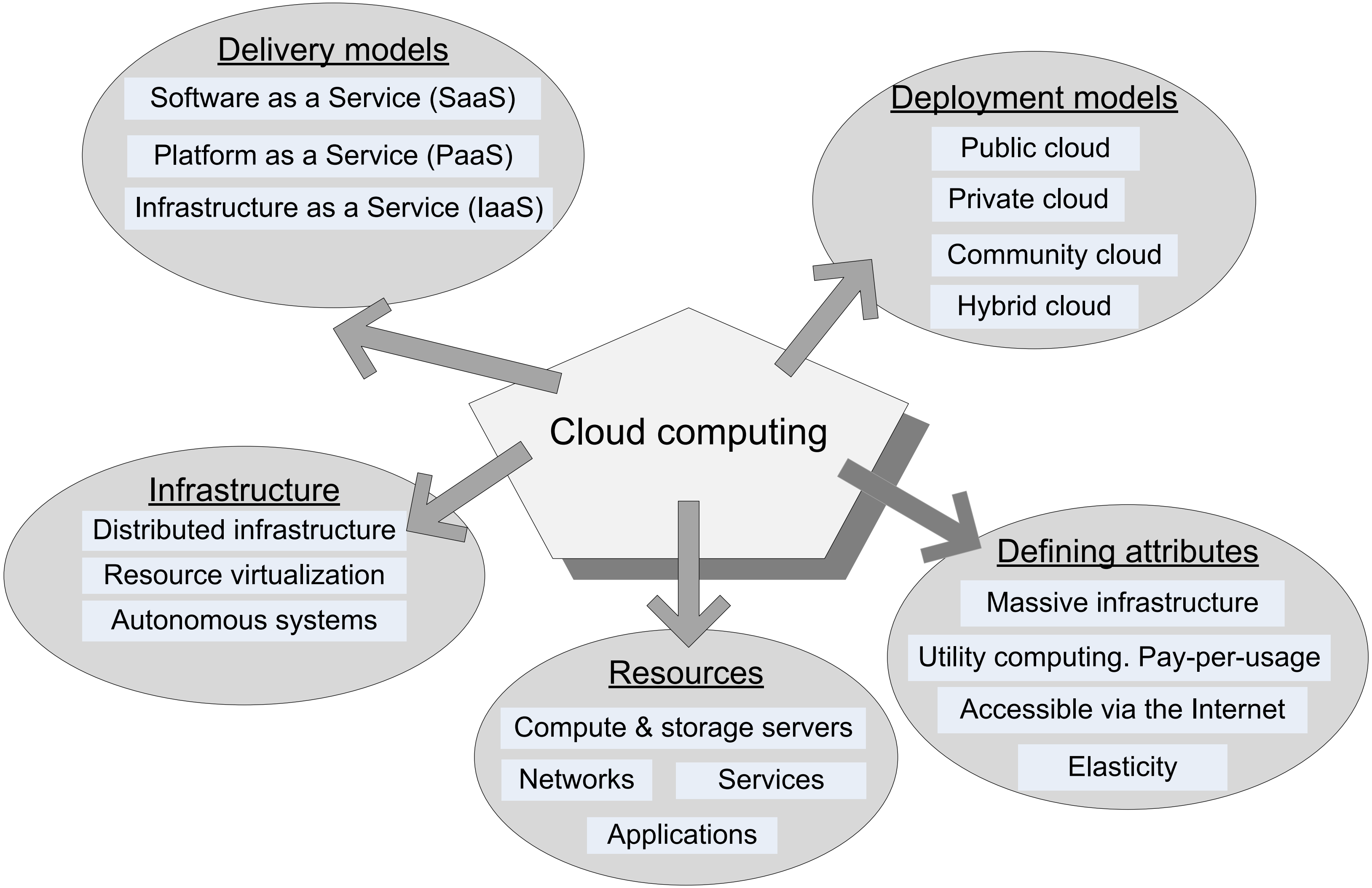
What is Cloud Computing?

- What do you think?

- *"**Cloud computing** is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility."* https://en.wikipedia.org/wiki/Cloud_computing

- *"Simply put, cloud computing is the delivery of computing services – servers, storage, databases, networking, software, analytics and more – over the Internet ("the cloud"). Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage, similar to how you're billed for gas or electricity at home." https://azure.microsoft.com/en-gb/overview/what-is-cloud-computing/*

Cloud Computing Models, Resources, Attributes



Early Models of Cloud Computing

- Basic reasoning: information and data processing can be done more efficiently on large farms of computing and storage systems accessible via the Internet.
- Two early models:

1. **Grid computing** – initiated by the National Labs in the early 1990s; targeted primarily at scientific computing.
   - *"Grid computing is the collection of computer resources from multiple locations to reach a common goal. The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files."* from Wikipedia
2. **Utility computing** – initiated in 2005-2006 by IT companies and targeted at enterprise computing.
   - *"Utility computing is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate."* from Wikipedia

Cloud computing - Characteristics

"*Cloud Computing offers on-demand, scalable and elastic computing (and storage services). The resources used for these services can be metered and users are charged only for the resources used.* " from the Book

Shared Resources and Resource Management:

1. Cloud uses a shared pool of resources
2. Uses Internet techn. to offer **scalable** and **elastic** services.
3. The term "**elastic computing**" refers to the ability of **dynamically** and **on-demand** acquiring computing resources and supporting a variable workload.
4. Resources are metered and users are charged accordingly.
5. It is more cost-effective due to **resource-multiplexing.** Lower costs for the cloud service provider are past to the cloud users.

Cloud computing (cont’ d)

Data Storage:

6. Data is stored:
    - in the “cloud”, in certain cases closer to the site where it is used.
    - appears to the users as if stored in a location-independent manner.
7. The data storage strategy can increase reliability, as well as security, and can lower communication costs.

Management:

8. The maintenance and security are operated by service providers.
9. The service providers can operate more efficiently due to specialisation and centralisation.

Cloud Computing Advantages

1. Resources, such as CPU cycles, storage, network bandwidth, are **shared.**

2. When multiple applications share a system, their peak demands for resources are not synchronised thus, **multiplexing** leads to a higher resource utilization.

3. Resources can be **aggregated** to support data-intensive applications.

4. Data sharing facilitates **collaborative** activities. Many applications require multiple types of analysis of shared data sets and multiple decisions carried out by groups scattered around the globe.

Cloud Computing Advantages

5. Eliminates the **initial investment costs** for a private computing infrastructure and the maintenance and operation costs.

6. **Cost reduction**: concentration of resources creates the opportunity to pay as you go for computing.

7. **Elasticity**: the ability to accommodate workloads with very large peak-to-average ratios.

8. **User convenience**: virtualization allows users to operate in familiar environments rather than in idiosyncratic ones.

Types of clouds

1. **Public Cloud** - the infrastructure is made available to the general public or a large industry group and is owned by the organization selling cloud services.

2. **Private Cloud** – the infrastructure is operated solely for an organization.

1. **Hybrid Cloud** - composition of two or more Clouds (public, private, or community) as unique entities but bound by a standardised technology that enables data and application portability.

2. **Other types: e.g., Community/Federated Cloud** - the infrastructure is shared by several organizations and supports a community that has shared concerns.

Why cloud computing is (could) be successful when other paradigms have failed?

- It is in a better position to exploit recent advances in software, networking, storage, and processor technologies promoted by the same companies who provide Cloud services.
- Economical reasons: It is used for enterprise computing; its adoption by industrial organizations, financial institutions, government, and so on has a huge impact on the economy.
- Infrastructures Management reasons:
  - A single Cloud consists of a mostly homogeneous (now more heterogeneous) set of hardware and software resources.
  - The resources are in a single administrative domain (AD). Security, resource management, fault-tolerance, and quality of service are less challenging than in a heterogeneous environment with resources in multiple ADs.

Challenges for cloud computing

1. Availability of service: what happens when the service provider cannot deliver?

2. Data confidentiality and auditability, a serious problem.

3. Diversity of services, data organization, user interfaces available at different service providers limit user mobility; once a customer is hooked to one provider it is hard to move to another.

4. Data transfer bottleneck; many applications are data-intensive.

More challenges

5. Performance unpredictability, one of the consequences of resource sharing.
   - How to use resource virtualization and performance isolation for QoS guarantees?
   - How to support elasticity, the ability to scale up and down quickly?

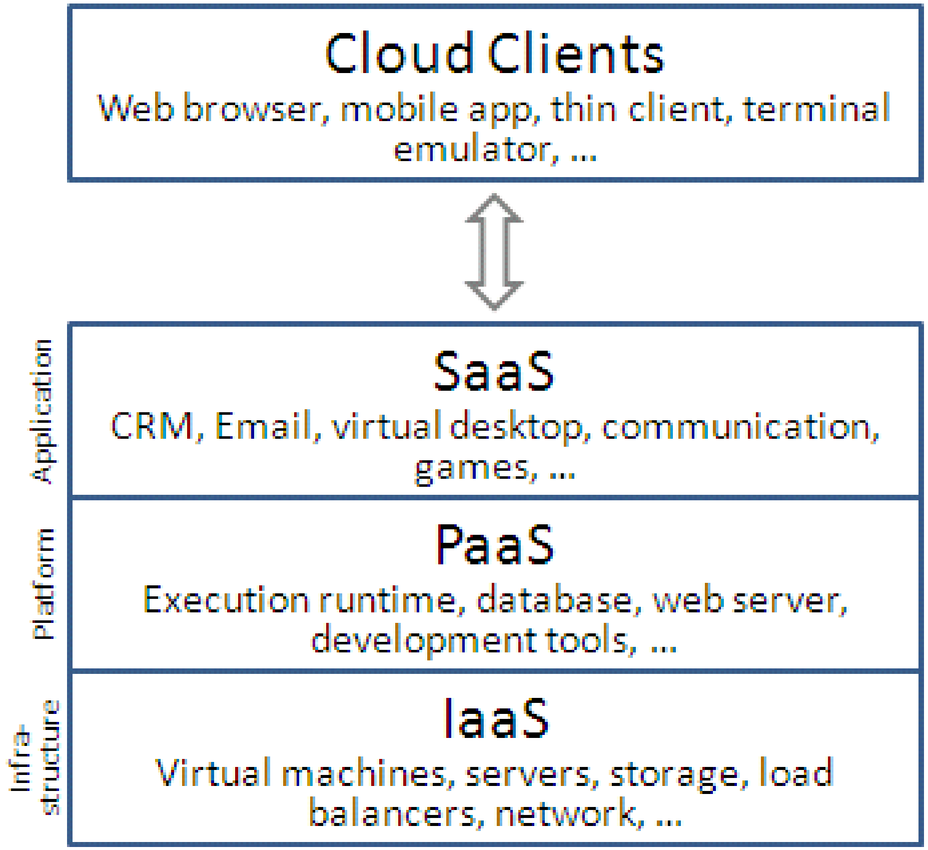
6. Resource management: It is a big challenge to manage different workloads running on large data centers. Are self-organization and self-management the solution?

7. Security and confidentiality: major concern for sensitive applications, e.g., healthcare applications.

Addressing these challenges is on-going work!

Cloud Delivery Models

1. **Software as a Service (SaaS)** (high level)
2. **Platform as a Service (PaaS)**
3. **Infrastructure as a Service (IaaS)** (low level)



Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...

SaaS
CRM, Email, virtual desktop, communication, games, ...

PaaS
Execution runtime, database, web server, development tools, ...

IaaS
Virtual machines, servers, storage, load balancers, network, ...

source Wikipedia

Infrastructure-as-a-Service (IaaS)

- Infrastructure is computal resources, CPU, VMs, storage, etc
- The user is able to deploy and run arbitrary software, which can include operating systems and applications.
- The user does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of some networking components, e.g., host firewalls.
- Services offered by this delivery model include: server hosting, storage, computing hardware, operating systems, virtual instances, load balancing, Internet access, and bandwidth provisioning.
- Example: Amazon EC2

Platform-as-a-Service (PaaS)

- Allows a cloud user to deploy consumer-created or acquired applications using programming languages and tools supported by the service provider.
- The user:
  - Has control over the deployed applications and, possibly, application hosting environment configurations.
  - Does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage.
- Not particularly useful when:
  - The application must be portable.
  - Proprietary programming languages are used.
  - The hardware and software must be customised to improve the performance of the application.
- Examples: Google App Engine, Windows Azure

Software-as-a-Service (SaaS)

- Applications are supplied by the service provider.
- The user does not manage or control the underlying Cloud infrastructure or individual application capabilities.
- Services offered include:
  - Enterprise services such as: workflow management, communications, digital signature, customer relationship management (CRM), desktop software, financial management, geo-spatial, and search.
- Not suitable for real-time applications or for those where data is not allowed to be hosted externally.

- Examples: Gmail, Salesforce

The Three delivery models of Cloud Computing

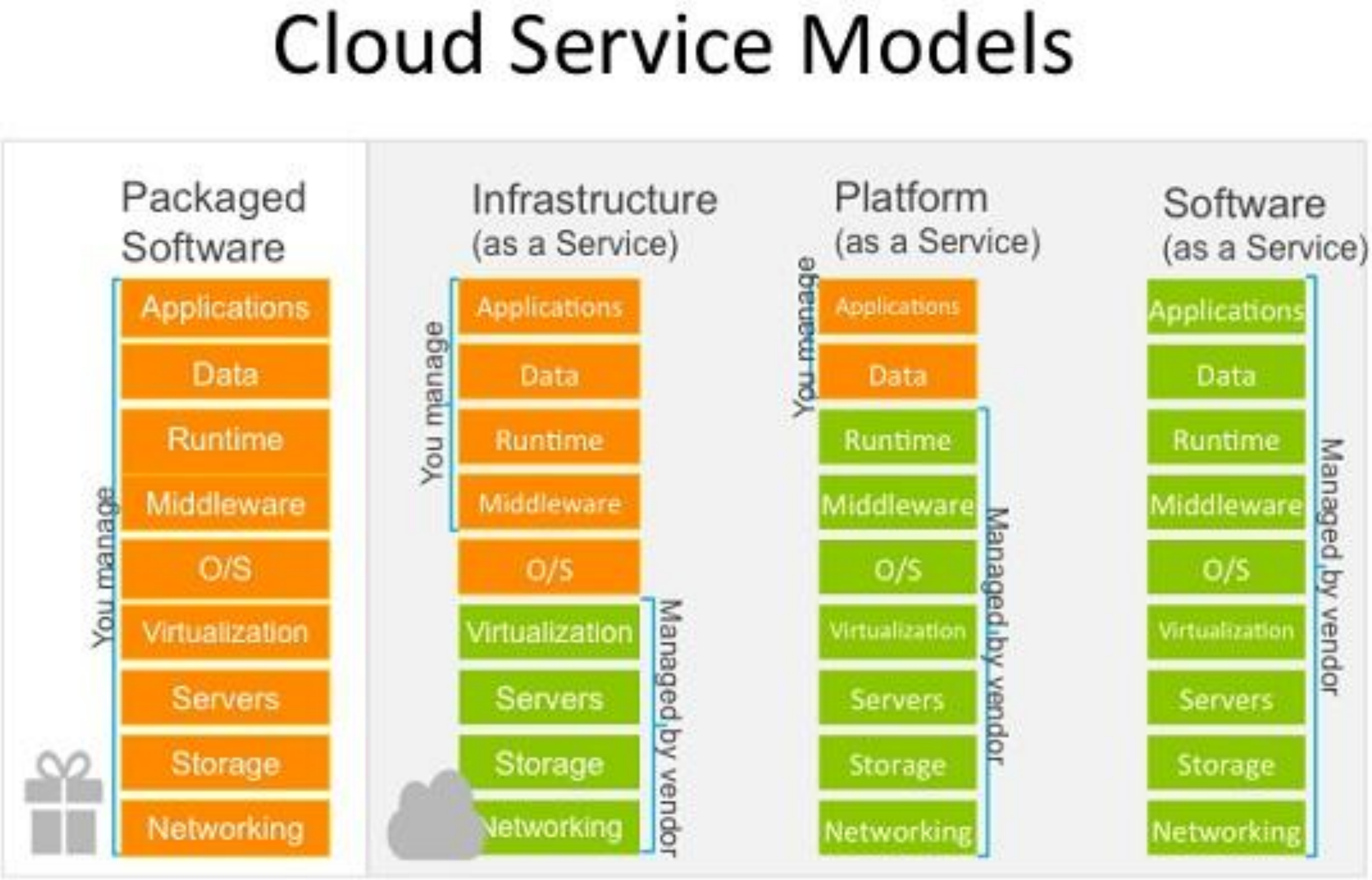


Figure 1. Source: Microsoft Azure

Cloud activities

- Service management and provisioning including:
  - Virtualization.
  - Service provisioning.
  - Call center.
  - Operations management.
  - Systems management.
  - QoS management.
  - Billing and accounting, asset management.
  - SLA management.
  - Technical support and backups.

Cloud activities (cont’ d)

- Security management including:
  - ID and authentication.
  - Certification and accreditation.
  - Intrusion prevention.
  - Intrusion detection.
  - Virus protection.
  - Cryptography.
  - Physical security, incident response.
  - Access control, audit and trails, and firewalls.

Cloud activities (cont’d)

- Customer services such as:
  - Customer assistance and on-line help.
  - Subscriptions.
  - Business intelligence.
  - Reporting.
  - Customer preferences.
  - Personalization.
- Integration services including:
  - Data management.
  - Development.

Ethical issues

- Paradigm shift with implications on computing ethics:
  - The control is relinquished to third party services.
  - Data is stored on multiple sites administered by several organizations.
  - Multiple services interoperate across the network.
- Implications:
  - Unauthorized access.
  - Data corruption.
  - Infrastructure failure, and service unavailability.

De-perimeterisation

- Systems can span the boundaries of multiple organizations and cross the security borders.

- The complex structure of Cloud services can make it difficult to determine who is responsible in case something undesirable happens.

- Identity fraud and theft are made possible by the unauthorised access to personal data in circulation and by new forms of dissemination through social networks and they could also pose a danger to Cloud Computing.

Privacy issues

- Cloud service providers have already collected petabytes of sensitive personal information stored in data centers around the world. The acceptance of Cloud Computing therefore will be determined by privacy issues addressed by these companies and the countries where the data centers are located.

- Privacy is affected by cultural differences; some cultures favour privacy, others emphasise community. This leads to an ambivalent attitude towards privacy in the Internet which is a global system.

Cloud Vulnerabilities

- Clouds are affected by malicious attacks and failures of the infrastructure, e.g., power failures.

- Such events can affect the Internet domain name servers and prevent access to a Cloud or can directly affect the Clouds:
  - in 2004 an attack at Akamai caused a domain name outage and a major blackout that affected Google, Yahoo, and other sites.
  - in 2009, Google was the target of a denial of service attack which took down Google News and Gmail for several days;
  - in 2012 lightning caused a prolonged down time at Amazon.

Characteristics

Cloud computing Characteristics

- 1. On-demand self-services
- 2. Rapid elasticity,
- 3. Resource pooling
- 4. Security
- 5. Sustainability
- 6. Flexible pricing models

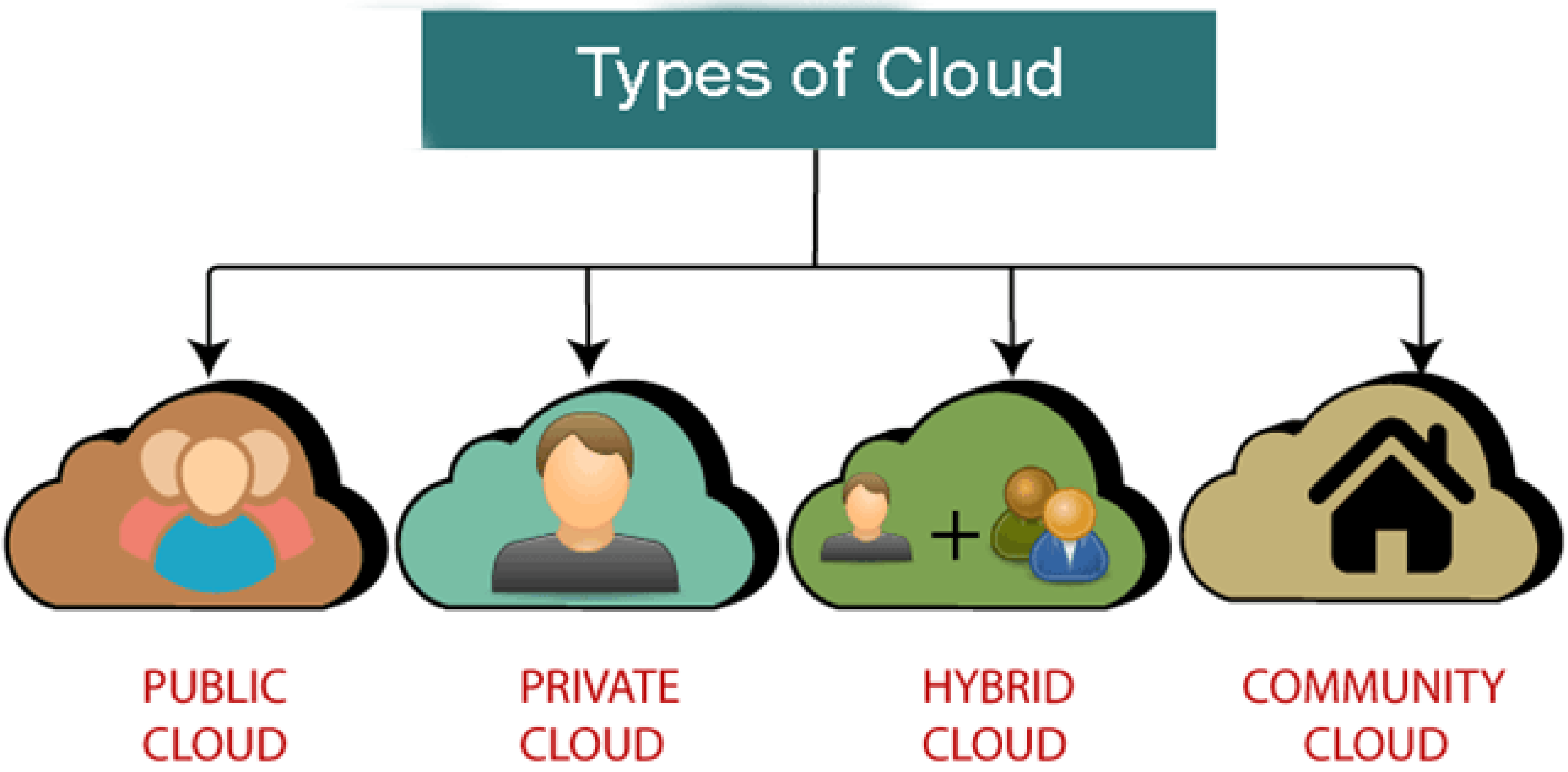
Characteristics

- Broad network access: The Computing services are generally provided over standard networks and heterogeneous devices.
- Measured service: The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.
- Multi-tenancy: Cloud computing providers can support multiple tenants (users or organizations) on a single set of shared resources.
- Virtualization: Cloud computing providers use virtualization technology to abstract underlying hardware resources and present them as logical resources to users.
- Resilient computing: Cloud computing services are typically designed with redundancy and fault tolerance in mind, which ensures high availability and reliability.
- Automation: Cloud computing services are often highly automated, allowing users to deploy and manage resources with minimal manual intervention.

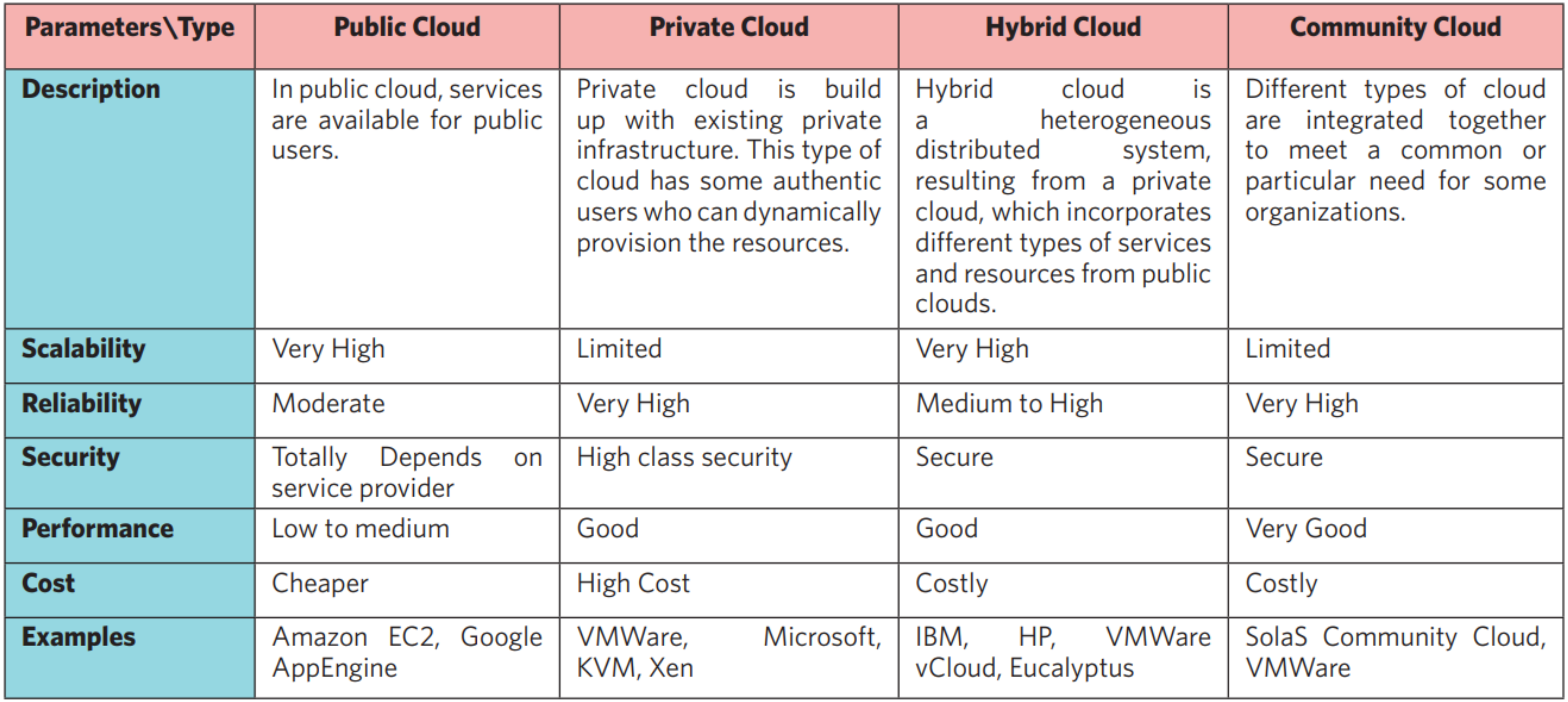
Characteristics

- Broad network access: The Computing services are generally provided over standard networks and heterogeneous devices.
- Measured service: The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.
- Multi-tenancy: Cloud computing providers can support multiple tenants (users or organizations) on a single set of shared resources.
- Virtualization: Cloud computing providers use virtualization technology to abstract underlying hardware resources and present them as logical resources to users.
- Resilient computing: Cloud computing services are typically designed with redundancy and fault tolerance in mind, which ensures high availability and reliability.
- Automation: Cloud computing services are often highly automated, allowing users to deploy and manage resources with minimal manual intervention.

Deployment Models



Deployment Models



Parameters\Type	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Description	In public cloud, services are available for public users.	Private cloud is build up with existing private infrastructure. This type of cloud has some authentic users who can dynamically provision the resources.	Hybrid cloud is a heterogeneous distributed system, resulting from a private cloud, which incorporates different types of services and resources from public clouds.	Different types of cloud are integrated together to meet a common or particular need for some organizations.
Scalability	Very High	Limited	Very High	Limited
Reliability	Moderate	Very High	Medium to High	Very High
Security	Totally Depends on service provider	High class security	Secure	Secure
Performance	Low to medium	Good	Good	Very Good
Cost	Cheaper	High Cost	Costly	Costly
Examples	Amazon EC2, Google AppEngine	VMWare, Microsoft, KVM, Xen	IBM, HP, VMWare vCloud, Eucalyptus	SolaS Community Cloud, VMWare

Deployment Models

Multicloud

- Multicloud is when an organization uses cloud computing services from at least two cloud providers to run their applications.
- Instead of using a single-cloud stack, multicloud environments typically include a combination of two or more public clouds, two or more private clouds, or some combination of both.
- By having the freedom to create a strategy that utilizes multiple vendors, you can pick and choose the capabilities that best suit your specific business needs and minimize vendor lock-in.

Deployment Models FAQs

Which cloud should I use?

That depends on what you're doing.

- Workloads with high volume or fluctuating demands might be better suited for a public cloud.
- Workloads with predictable use patterns might be better off in a private cloud.
- Hybrid clouds are the catch-all, because any workload can be hosted anywhere.

Which cloud is safest?

- Public clouds tend to have a wider variety of security threats due to multi-tenancy and numerous access points. Public clouds often split security responsibilities. For instance, infrastructural security can be the provider's responsibility, while workload security can be the tenant's responsibility.
- Private clouds are thought to be more secure because workloads usually run behind the user's firewall, but that all depends on how strong your own security is.
- Hybrid cloud security comprises the best features of every environment, where users and admins can minimize data exposure by moving workloads and data across environments based on compliance, audit, policy, or security requirements.

Deployment Models FAQs

Which cloud costs more?

- You usually pay for what you use in a public cloud, though some public clouds (like the Massachusetts Open Cloud) don't charge tenants.
- Whoever set up a private cloud is usually responsible for purchasing or renting new hardware and resources to scale up.
- Hybrid clouds can include any on-prem, off-prem, or provider's cloud to create a custom environment that suits your cost requirements.

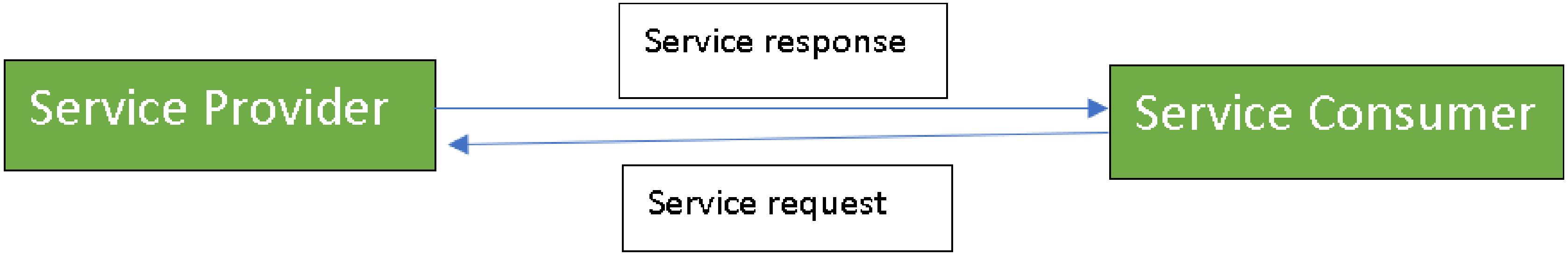
Which cloud has the best resources?

That depends on how you want to spend money. Do you want to incur capital expenses (CapEx) or operating expenses (OpEx)? This is the classic *scale-up* vs. *scale-out* question.

- Public cloud users seem to have unlimited access to resources, but accessing those resources is usually an operational expense.
- Deploying more private cloud resources requires buying or renting more hardware—all capital expenses.
- Hybrid clouds give you the option of using operating expenses to scale out or capital expenses to scale up.

Cloud Computing Architecture

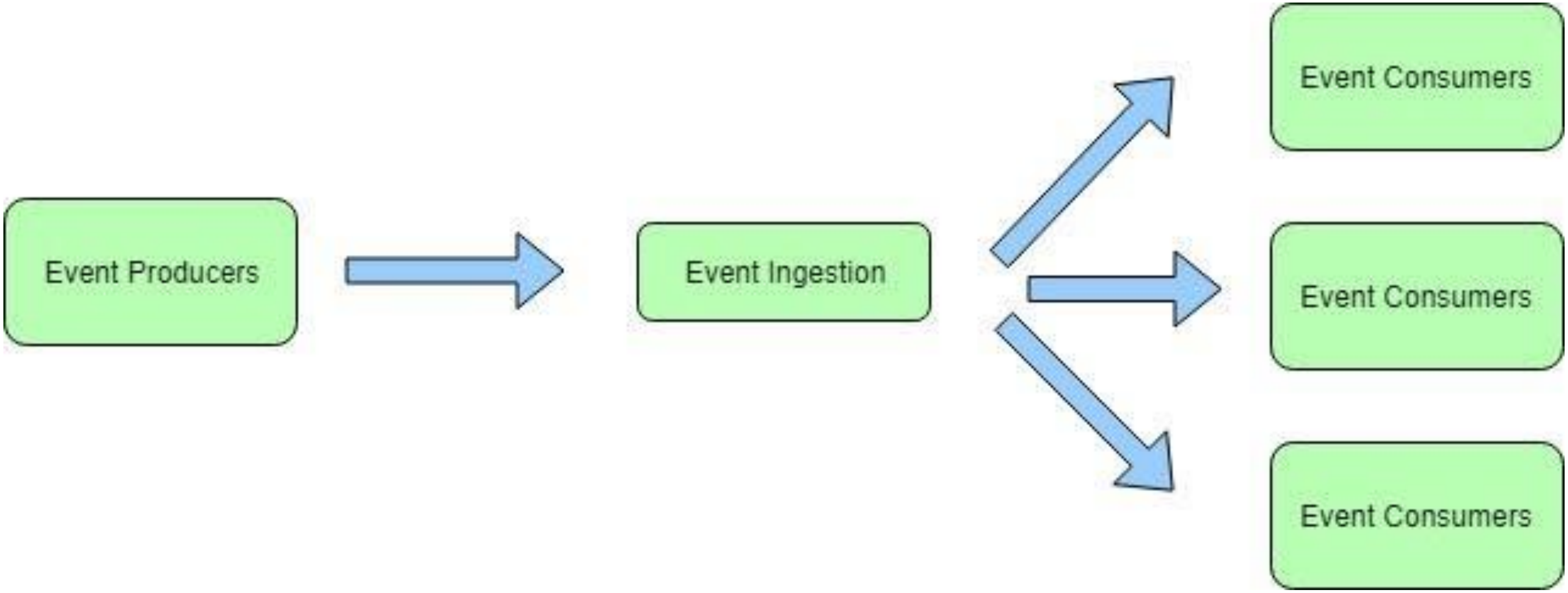
Architecture of cloud computing is the combination of both SOA (Service Oriented Architecture) and EDA (Event Driven Architecture). Client infrastructure, application, service, runtime cloud, storage, infrastructure, management, and security all these are the components of cloud computing architecture.



Service-Oriented Architecture (SOA)

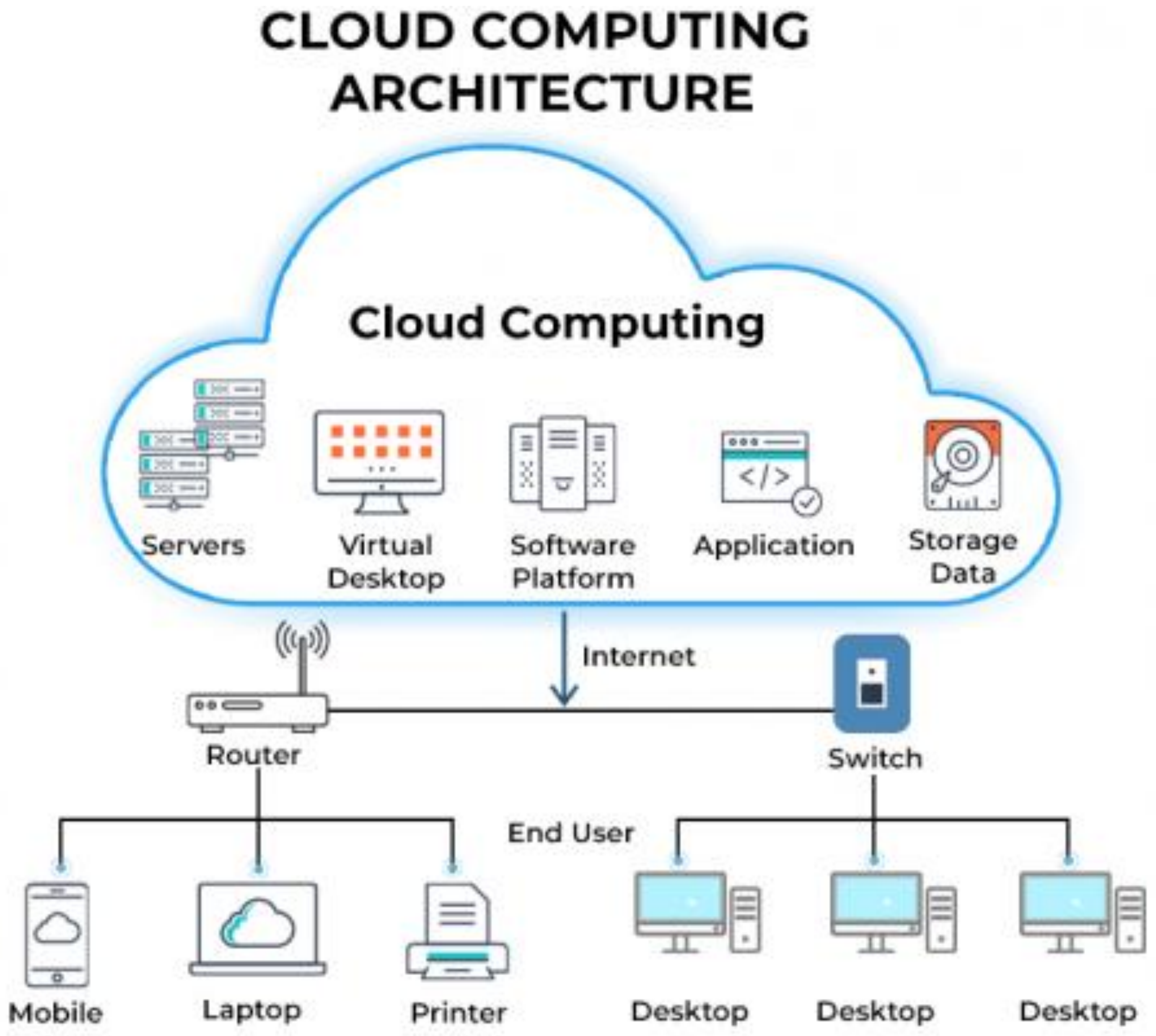
- **Service provider:** The service provider is the maintainer of the service and the organization that makes available one or more services for others to use. To advertise services, the provider can publish them in a registry, together with a service contract that specifies the nature of the service, how to use it, the requirements for the service, and the fees charged.
- **Service consumer:** The service consumer can locate the service metadata in the registry and develop the required client components to bind and use the service.

Cloud Computing Architecture



Event-Driven Architecture (EDA)

Cloud Computing Architecture



Cloud Computing Architecture

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

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

Cloud Computing Architecture

Back End

- Application – Application in backend refers to a software or platform to which client accesses. Means it provides the service in backend as per the client requirement.
- Service – Service in backend refers to the major three types of cloud based services like SaaS, PaaS and IaaS. Also manages which type of service the user accesses.
- Runtime Cloud- Runtime cloud in backend provides the execution and Runtime platform/environment to the Virtual machine.
- Storage – Storage in backend provides flexible and scalable storage service and management of stored data.
- Infrastructure – Cloud Infrastructure in backend refers to the hardware and software components of cloud like it includes servers, storage, network devices, virtualization software etc.

Cloud Computing Architecture

- Management – Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.
- Security – Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, and infrastructure to end-users.
- Database– Database in backend refers to provide database for storing structured data, such as SQL and NOSQL databases. Example of Databases services include Amazon RDS, Microsoft Azure SQL database and Google CLoud SQL.
- Networking– Networking in backend services that provide networking infrastructure for application in the cloud, such as load balancing, DNS and virtual private networks.
- Analytics– Analytics in backend service that provides analytics capabillities for data in the cloud, such as warehousing, bussness intellegence and machine learning.

Cloud Computing Infrastructure

- Cloud infrastructure is a term used to describe the components needed for cloud computing, which includes hardware, abstracted resources, storage, and network resources.
- Think of cloud infrastructure as the tools needed to build a cloud. In order to host services and applications in the cloud, you need cloud infrastructure.

How does cloud infrastructure work?

An abstraction technology or process—like virtualization—is used to separate resources from physical hardware and pool them into clouds; automation software and management tools allocate these resources and provision new environments so users can access what they need—when they need it.

Cloud Computing Infrastructure

What's included in cloud infrastructure?

Cloud infrastructure is made up of several components, each integrated with one another into a single architecture supporting business operations. A typical solution may be composed of

- Hardware
- Virtualization
- Storage
- Networking components

Cloud Computing Infrastructure

What's included in cloud infrastructure?

Hardware

- Although you probably think of clouds as being virtual, they require hardware as part of the infrastructure.
- A cloud network is made up of a variety of physical hardware that can be located at multiple geographical locations.
- The hardware includes networking equipment, like switches, routers, firewalls, and load balancers, storage arrays, backup devices, and servers.
- Virtualization connects the servers together, dividing and abstracting resources to make them accessible to users.

Cloud Computing Infrastructure

What's included in cloud infrastructure?

Virtualization

- Virtualization is technology that separates IT services and functions from hardware.
- Software called a hypervisor sits on top of physical hardware and abstracts the machine's resources, such as memory, computing power, and storage.
- Once these virtual resources are allocated into centralized pools they’re considered clouds.
- With clouds, you get the benefits of self-service access, automated infrastructure scaling, and dynamic resource pools.

Cloud Computing Infrastructure

What's included in cloud infrastructure?

Storage

- Within a single datacenter, data may be stored across many disks in a single storage array. Storage management ensures data is correctly being backed up, that outdated backups are removed regularly, and that data is indexed for retrieval in case any storage component fails.
- Virtualization abstracts storage space from hardware systems so that it can be accessed by users as cloud storage.
- When storage is turned into a cloud resource, you can add or remove drives, repurpose hardware, and respond to change without manually provisioning separate storage servers for every new initiative.

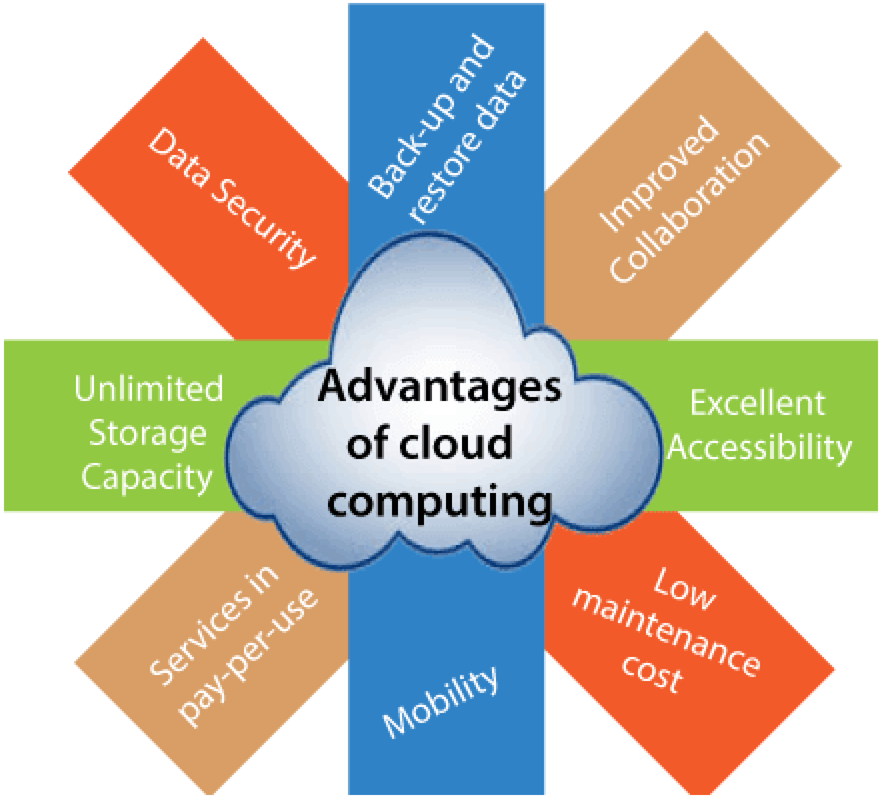
Cloud Computing Infrastructure

What's included in cloud infrastructure?

Network

- The network is composed of physical wires, switches, routers, and other equipment. Virtual networks are created on top of these physical resources.
- A typical cloud network configuration is composed of multiple subnetworks, each with varying levels of visibility. The cloud permits the creation of virtual local area networks (VLANs) and assigns static and/or dynamic addresses as needed for all network resources.
- The cloud resources are delivered to users over a network, such as the internet or an intranet, so you can access cloud services or apps remotely on demand.

Cloud Computing Advantages



Cloud Computing Advantages

1) 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.

Cloud Computing Advantages

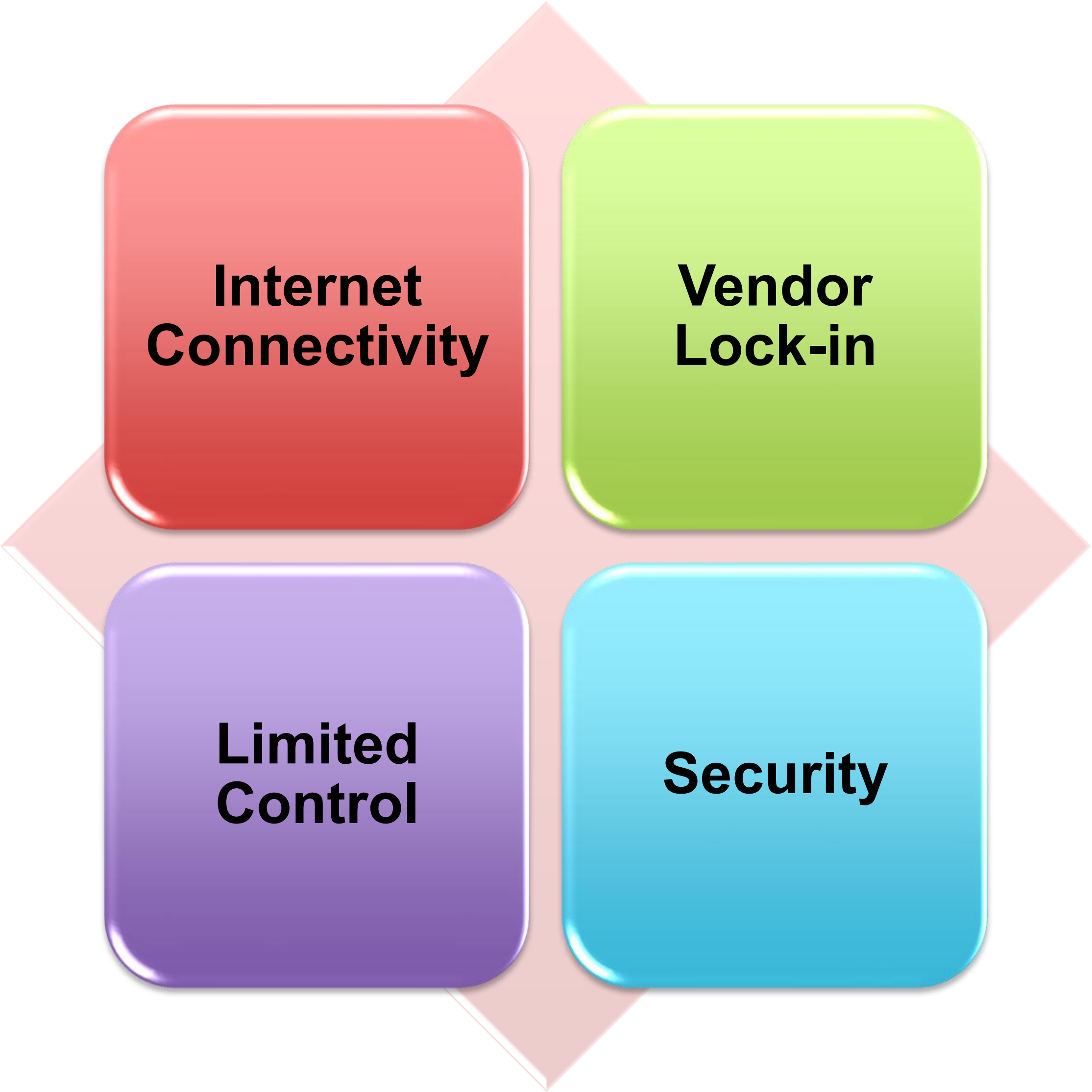
5) Mobility
Cloud computing allows us to easily access all cloud data via mobile.

6) Services 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.

Cloud Computing Disadvantages



Internet Connectivity

Vendor Lock-in

Limited Control

Security

Cloud Computing Disadvantages

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.

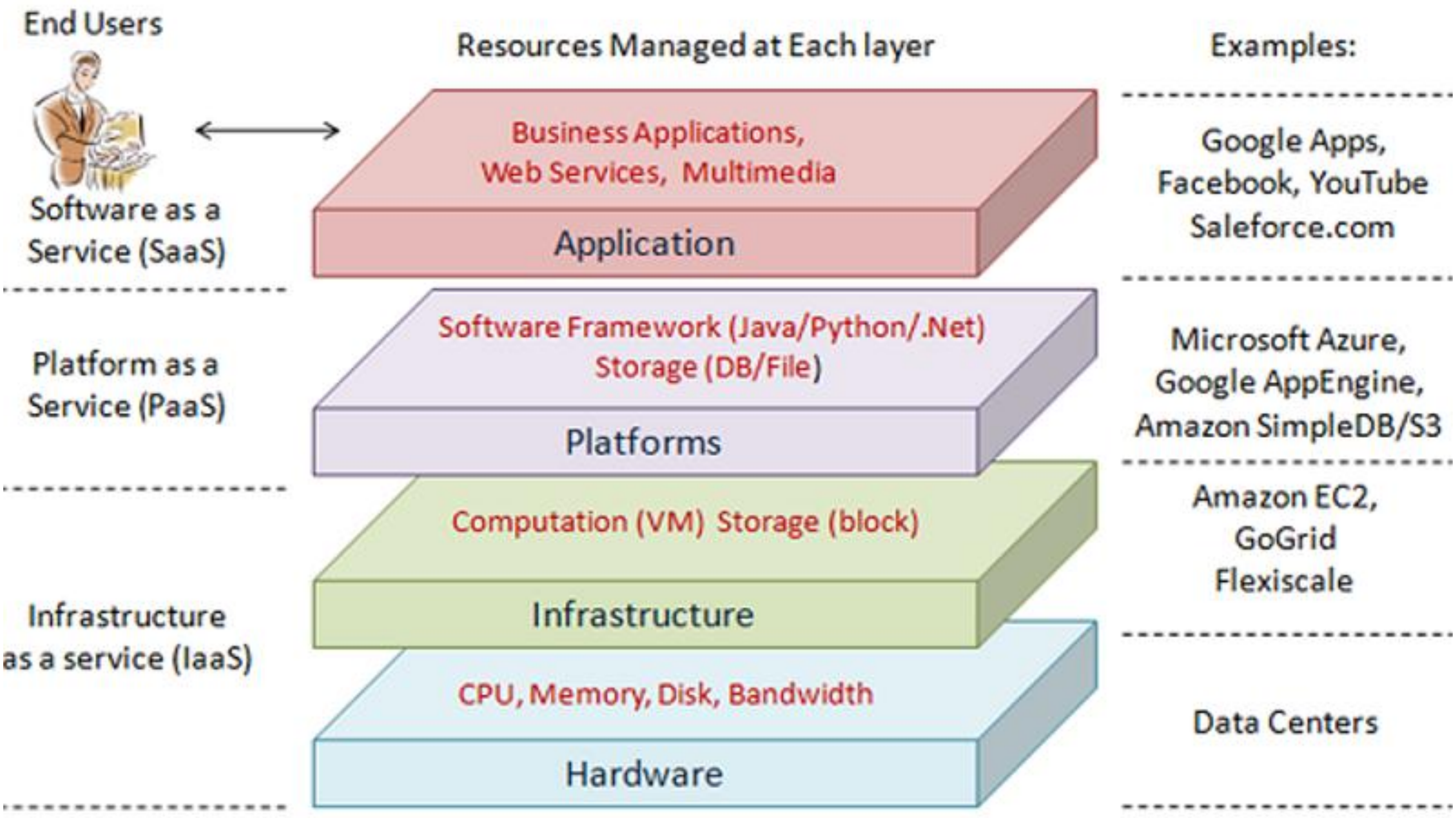
3) Limited Control

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

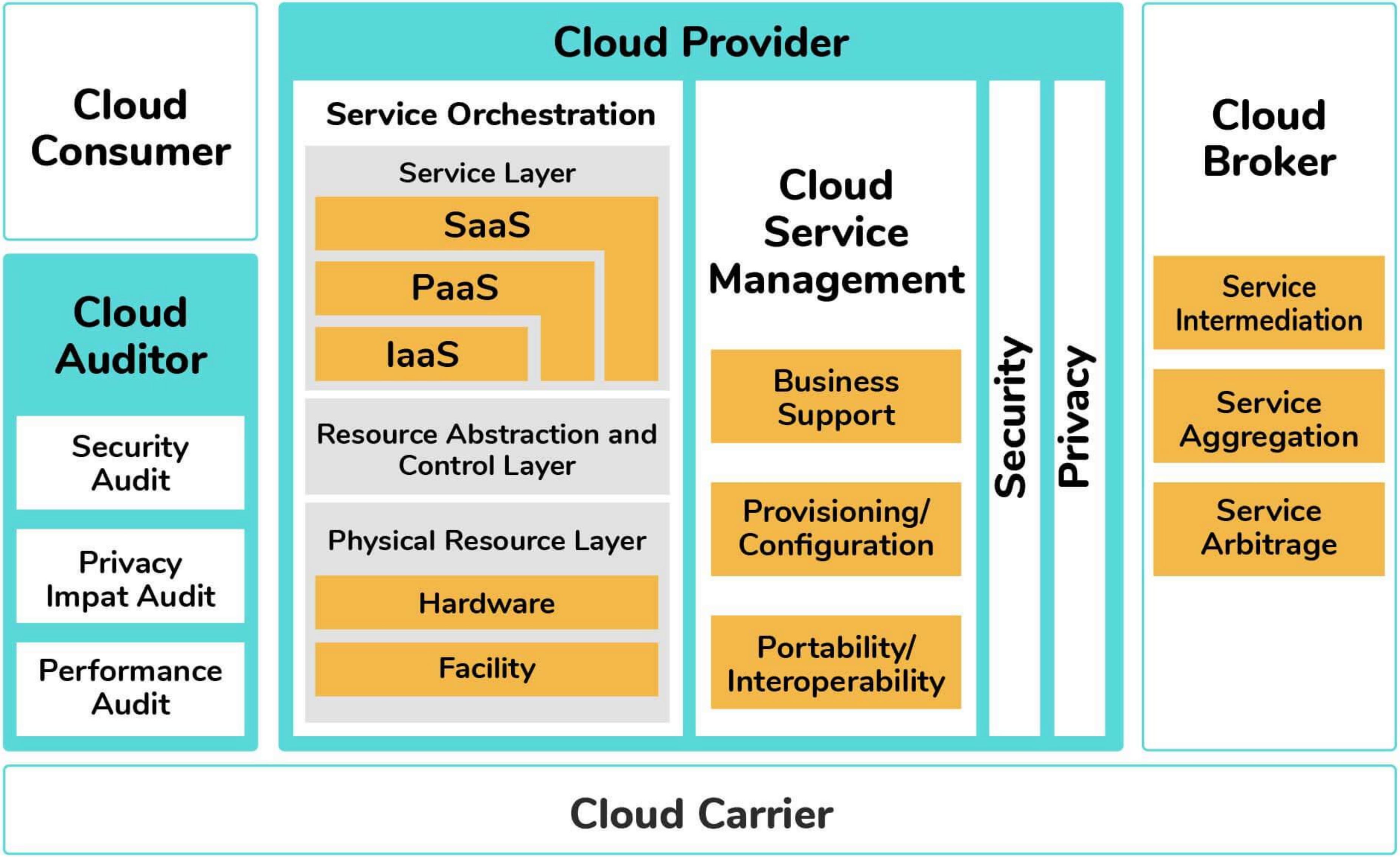
Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.

Cloud Computing Layered Architecture



- The Hardware Layer-Data center
- The Infrastructure Layer
- The Platform Layer
- The Application Layer

Cloud Computing Layered Architecture



Virtualization

Virtualization in Cloud Computing

- **Virtualization** is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".
- In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

Types of Virtualization

- Hardware Virtualization.
- Operating system Virtualization.
- Server Virtualization.
- Storage Virtualization.

Cloud Computing

Xaas in Cloud Computing

- "**Anything as a service**" (XaaS) describes a general category of cloud computing and remote access services. It recognizes the vast number of products, tools, and technologies now delivered to users as a service over the Internet.
- Essentially, any IT function can be a service for enterprise consumption. The service is paid for in a flexible consumption model rather than an advance purchase or license.

DaaS in Cloud Computing

- Desktop as a Service (DaaS) is a cloud computing offering where a service provider distributes virtual desktops to end-users over the Internet, licensed with a per-user subscription.
- The provider takes care of backend management for small businesses that find their virtual desktop infrastructure to be too expensive or resource-consuming. This management usually includes maintenance, backup, updates, and data storage. Cloud service providers can also handle security and applications for the desktop, or users can manage these service aspects individually.

Cloud Computing

Container as a Service (CaaS) in Cloud Computing

What is a Container?

- A container is a useful unit of software into which application code and libraries and their dependencies can be run anywhere, whether on a desktop, traditional IT, or in the cloud.
- To do this, containers take advantage of virtual operating systems (OS) in which OS features (in the Linux kernel, which are groups of first names and domains) are used in CPU partitions, memory, and disk access.

Container as a Service (CaaS):

- A container as a Service (CaaS) is a cloud service model that allows users to upload, edit, start, stop, rate, and otherwise manage containers, applications and collections. It enables these processes through tool-based virtualization, a programming interface (API), or a web portal interface. CaaS helps users build rich, secure, segmented applications through local or cloud data centers. Containers and collections are used as a service with this model and installed on-site in the cloud or data centers.
- CaaS assists development teams in deploying and managing systems efficiently while providing more control of container orchestration than is permitted by PaaS.

Cloud Computing

Container as a Service (CaaS) in Cloud Computing

What is a Container?

- A container is a useful unit of software into which application code and libraries and their dependencies can be run anywhere, whether on a desktop, traditional IT, or in the cloud.
- To do this, containers take advantage of virtual operating systems (OS) in which OS features (in the Linux kernel, which are groups of first names and domains) are used in CPU partitions, memory, and disk access.

Container as a Service (CaaS):

- A container as a Service (CaaS) is a cloud service model that allows users to upload, edit, start, stop, rate, and otherwise manage containers, applications and collections. It enables these processes through tool-based virtualization, a programming interface (API), or a web portal interface. CaaS helps users build rich, secure, segmented applications through local or cloud data centers. Containers and collections are used as a service with this model and installed on-site in the cloud or data centers.
- CaaS assists development teams in deploying and managing systems efficiently while providing more control of container orchestration than is permitted by PaaS.

Cloud Computing

What are Microservices?

Microservices is a process of developing applications that consist of code that is independent of each other and of the underlying developing platform. Each microservice runs a unique process and communicates through well-defined and standardized APIs, once created. These services are defined in the form of a catalog so that developers can easily locate the right service and also understand the governance rules for usage.

Why are microservices important for a true cloud environment?

The reason why microservices are so important for a true cloud environment is because of these four key benefits:

- Each microservice is built to serve a specific and limited purpose, and hence application development is simplified. Small development teams can then focus on writing code for some of the narrowly defined and easily understood functions.
- Code changes will be smaller and less complex than with a complex integrated application, making it easier and faster to make changes, whether to fix a problem or to upgrade service with new requirements.
- Scalability — Scalability makes it easier to deploy an additional instance of a service or change that service as needs evolve.
- Microservices are fully tested and validated. When new applications leverage existing microservices, developers can assume the integrity of the new application without the need for continual testing.

Cloud Computing

What are Cloud-Native Applications?

‘Cloud native’ is a software framework designed with containers, microservices, dynamic orchestration, and also continuous delivery of software. Every part of the cloud-native application has within it its own container and is dynamically orchestrated with other containers to optimize the way the resources are utilized