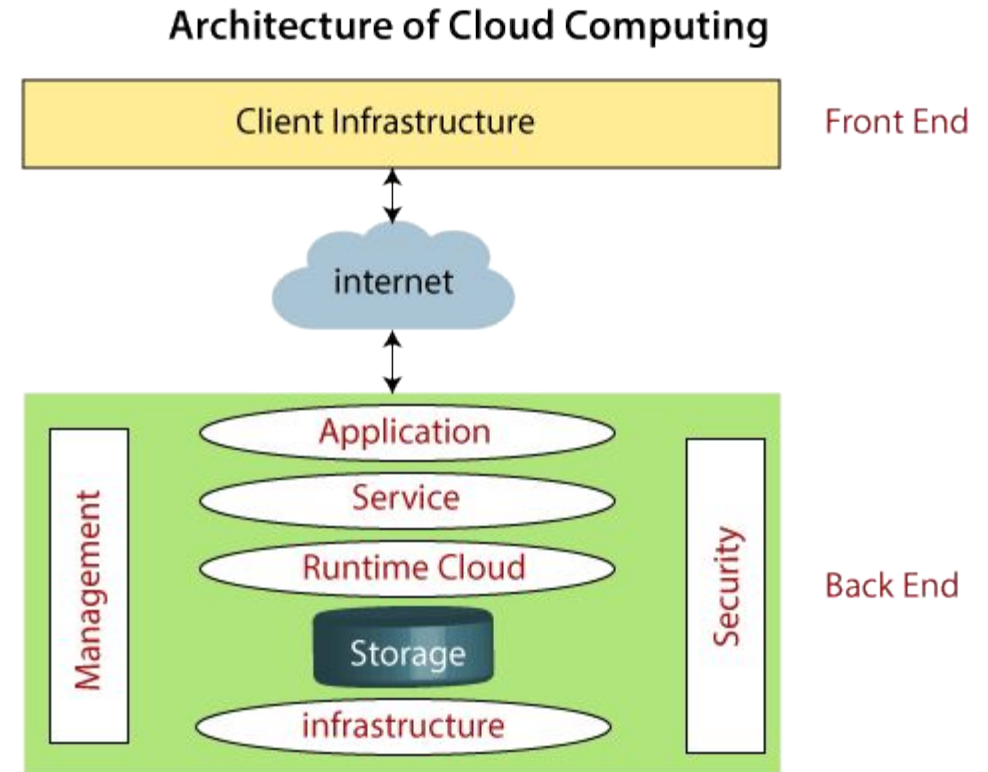


Cloud Architecture

Cloud Types: Private Cloud, Public cloud, Hybrid cloud, community cloud. Cloud Computing Service Models (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Anything as a Service (XaaS)) Service model comparison, Service model selection criteria, Responsibilities in each service model

Intro

- Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**.
- Cloud computing architecture is divided into the following two parts -
 - Front End
 - Back End
- The below diagram shows the architecture of cloud computing -



Structure

Front-End

- It provides applications and the interfaces that are required for the cloud-based service.
- It consists of client's side applications, which are web browsers such as Google Chrome and Internet Explorer.
- Cloud infrastructure is the only component of the front-end. Let's understand it in detail.
- Cloud infrastructure consists of hardware and software components such as data storage, server, virtualization software, etc.
- It also provides a Graphical User Interface to the end-users to perform respective tasks.

Back-End

It is 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

Application

- It can either be a software or a platform
- Depending upon the client requirement, the application provides the result to the end-user (with resources) in the back end

Service

- Service is an essential component in cloud architecture
- Its responsibility is to provide utility in the architecture
- In a Cloud, few widely used services among the end-users are storage application development environments and web services

Storage

- It stores and maintains data like files, videos, documents, etc. over the internet
- Some of the popular examples of storage services are below:
 - Amazon S3, Oracle Cloud-Storage, Microsoft Azure Storage
- Its capacity varies depending upon the service providers available in the market

Management

- Its task is to allot specific resources to a specific task, it simultaneously performs various functions of the cloud environment
- It helps in the management of components like application, task, service, security, data storage, and cloud infrastructure
- In simple terms, it establishes coordination among the cloud resources

Security

- Security is an integral part of back-end cloud infrastructure
- It provides secure cloud resources, systems, files, and infrastructure to end-users
- Also, it implements security management to the cloud server with virtual firewalls which results in preventing data loss

Benefits of Cloud Computing Architecture

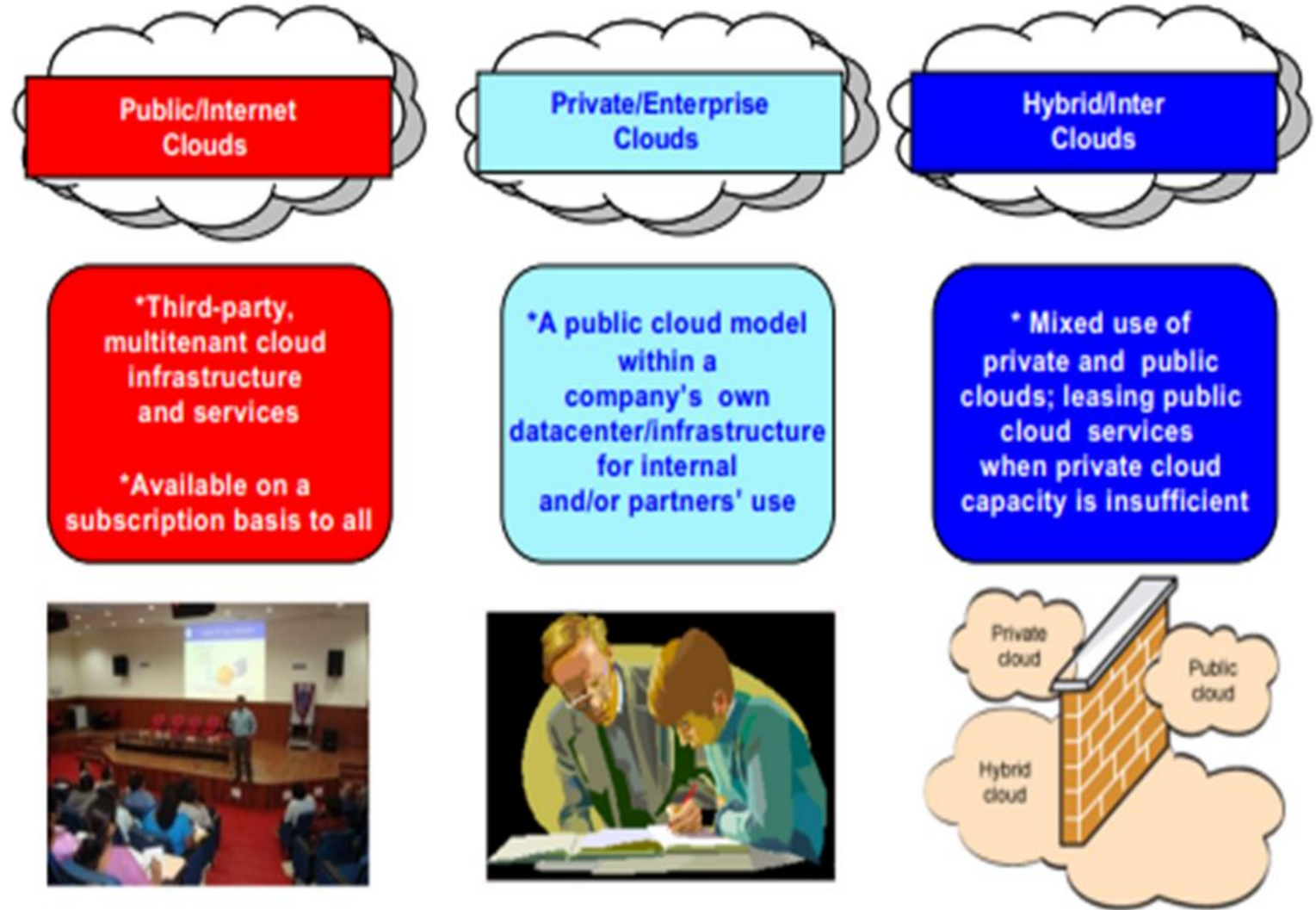
- It solves latency issues and improves data processing requirements
- It reduces IT operating costs and gives good accessibility to access data and digital tools
- It helps businesses to easily scale up and scale down their cloud resources
- It has a flexibility feature which gives businesses a competitive advantage
- It results in better disaster recovery and provides high security
- It automatically updates its services
- It encourages remote working and promotes team collaboration

Cloud Types

- Every cloud abstracts, pools, and shares scalable computing resources across a network. Every cloud type also enables cloud computing, which is the act of running workloads within that system.
- And every cloud is created using a unique mix of technologies, which almost always includes an operating system, some kind of management platform, and application programming interfaces (APIs).
- Virtualization and automation software can also be added to every kind of cloud for additional capabilities or increased efficiencies.

Cloud Deployment Models

1. public clouds
2. private/enterprise clouds
3. hybrid clouds



Public Cloud

- A public cloud is a cloud service offered to multiple customers by a cloud provider.
- The term "public cloud" is used to differentiate between the original cloud model of services accessed over the Internet and the private cloud model.
- Public clouds include SaaS, PaaS, and IaaS services.



Cloud Types: Public Cloud

- Public clouds are a type of cloud computing **run by a third-party cloud provider.**
- These cloud providers **deliver cloud services to their clients over the public internet.**
- A cloud **provider keeps ownership and control of the cloud storage, hardware, infrastructure and resources.**
- This means that the cloud **provider typically handles any updates or issues** that require troubleshooting.
- Some public clouds give their clients free use of their cloud services. Other public clouds use a **tiered subscription system** where clients can choose how much storage and other cloud resources they need.
- Since public clouds **offer shared resources to multiple clients**, they're usually the most cost-efficient type of cloud deployment.

Cloud Types: Public Cloud

- Public cloud operated on the **pay-as-per-use model and administrated by the third party**, i.e., Cloud service provider.
- In the Public cloud, the **same storage is being used by multiple users** at the same time.
- Public cloud is **owned, managed, and operated by businesses, universities, government organizations, or a combination of them.**
- Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM's Blue Cloud, Sun Cloud, and Google Cloud are examples of the public cloud.

When to use the public cloud

- Predictable computing needs, such as **communication services for a specific number of users**
- Apps and services necessary to **perform IT and business operations**
- Additional resource requirements **to address varying peak demands**
- Software **development and test environments**

Advantages of Public Cloud

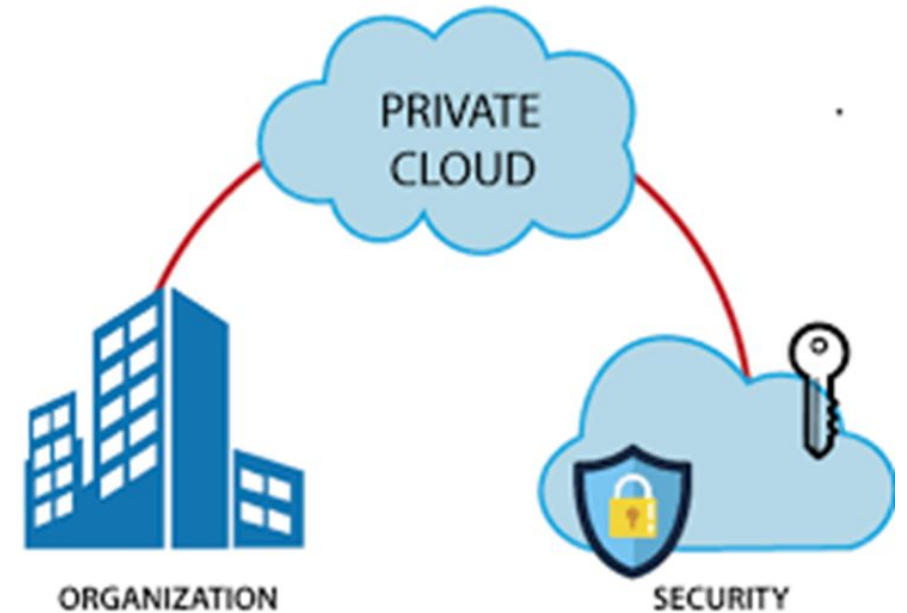
- **Low Cost:** Public cloud has a lower cost than private, or hybrid cloud, as it shares the same resources with a large number of consumers.
- **Location Independent:** Public cloud is location independent because its services are offered through the internet.
- **Save Time:** In Public cloud, the cloud service provider is responsible for the manage and maintain data centers in which data is stored, so the cloud user can save their time to establish connectivity, deploying new products, release product updates, configure, and assemble servers.
- **Quickly and easily set up:** Organizations can easily buy public cloud on the internet and deployed and configured it remotely through the cloud service provider within a few hours.
- **Business Agility:** Public cloud provides an ability to elastically re-size computer resources based on the organization's requirements.
- **Scalability and reliability:** Public cloud offers scalable (easy to add and remove) and reliable (24*7 available) services to the users at an affordable cost.

Disadvantages of Public Cloud

- **Low Security:** Public Cloud is less secure because resources are shared publicly.
- **Performance:** In the public cloud, performance depends upon the speed of internet connectivity.
- **Less customizable:** Public cloud is less customizable than the private cloud.

Private Cloud

- Private cloud is a cloud computing environment dedicated to a single customer.
- It combines many of the benefits of cloud computing with the security and control of on-premises IT infrastructure.



When to use the private cloud

- Highly regulated industries and government agencies
- Sensitive data
- Companies that require strong control and security over their IT workloads and the underlying infrastructure
- Large enterprises that require advanced data center technologies to operate efficiently and cost-effectively
- Organizations that can afford to invest in high performance and availability technologies

Cloud Types: Private Cloud

- Only one **individual or business** uses the resources and storage of a private cloud.
- Users **access private cloud services over a private network that others can't access from the public internet.**
- Private clouds can be **physically located on a company's premises.**
- Some third-party cloud providers may also **offer clients a private cloud option for a higher price than a public cloud.**
- Since private clouds **don't share their resources with multiple clients** over the internet, private clouds can offer organizations greater security than a public cloud.
- However, a private cloud typically **costs more than a public one.**

Advantages of private cloud

- 1.Exclusive environments.**
- 2.Custom security.**
- 3.Scalability without tradeoffs.**
- 4.Efficient performance.**
- 5.Flexibility.**

Drawbacks of private cloud

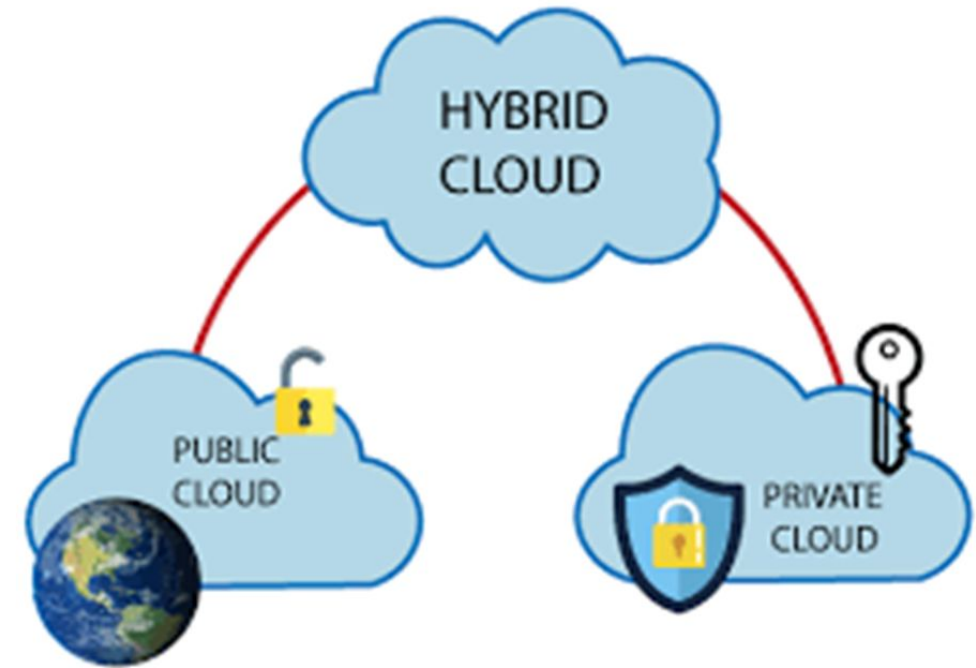
1.Price.

2.Mobile difficulty.

3.Scalability depends.

hybrid cloud

- The hybrid cloud is any cloud infrastructure environment that combines both public and private cloud solutions.



Cloud Types: Hybrid Cloud

- A hybrid cloud **combines services of both public and private clouds**. With a hybrid cloud, organizations can **typically choose to combine various elements of both types of clouds**.
- Since organizations can often customize hybrid clouds, this type of cloud deployment **gives companies greater flexibility in their infrastructure and operations**.
- For example, an organization may use aspects of a private cloud **to keep their confidential business data secure**, but use elements of public clouds for normal file-sharing or document collaboration.
- As another example, a company might create a hybrid cloud with primarily public cloud functions for their marketing and sales staff, but that mainly operates as a private cloud for their IT and accounting departments.

Cloud Types: Hybrid Cloud

- Hybrid cloud is a combination of **public and private** clouds.
Hybrid cloud = public cloud + private cloud
- The main aim to combine these cloud (Public and Private) is to create a unified, automated, and well-managed computing environment.
- In the Hybrid cloud, **non-critical activities** are performed by the **public cloud** and **critical activities** are performed by the **private cloud**.
- Mainly, a hybrid cloud is used in finance, healthcare, and Universities.
- The best hybrid cloud provider companies are **Amazon, Microsoft, Google, Cisco, and NetApp**.

When to use the hybrid cloud

- **Organizations serving multiple verticals facing different IT security, regulatory, and performance requirements**
- **Optimizing cloud investments without compromising on the value that public or private cloud technologies can deliver**
- **Improving security** on existing cloud solutions such as SaaS offerings that must be delivered via secure private networks
- **Strategically approaching cloud investments to continuously switch and tradeoff between the best cloud service delivery model available in the market**

Cloud Types: Hybrid Cloud

- Advantages of Hybrid Cloud

1) **Flexible and secure:** It provides flexible resources because of the public cloud and secure resources because of the private cloud.

2) **Cost effective:** Hybrid cloud costs less than the private cloud. It helps organizations to save costs for both infrastructure and application support.

3) **Cost effective:** It offers the features of both the public as well as the private cloud. A hybrid cloud is capable of adapting to the demands that each company needs for space, memory, and system.

4) **Security:** Hybrid cloud is secure because critical activities are performed by the private cloud.

5) **Risk Management:** Hybrid cloud provides an excellent way for companies to manage the risk.

Cloud Types: Hybrid Cloud

Disadvantages of Hybrid Cloud

- 1) **Networking issues:** In the Hybrid Cloud, networking becomes complex because of the private and the public cloud.
- 2) **Infrastructure Compatibility:** Infrastructure compatibility is the major issue in a hybrid cloud. With dual-levels of infrastructure, a private cloud controls the company, and a public cloud does not, so there is a possibility that they are running in separate stacks.
- 3) **Reliability:** The reliability of the services depends on cloud service providers.

Cloud Types: Community Cloud

- Community cloud is a cloud infrastructure that allows systems and services to **be accessible by a group of several organizations to share the information**. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.
- It is **owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them**. Example: Our government organization within India may share computing infrastructure in the cloud to manage data.
- **Example:** Our government organization within India may share computing infrastructure in the cloud to manage data.

Cloud Types: Community Cloud

Advantages of Community Cloud

- **Cost effective:** Community cloud is cost effective because the whole cloud is shared between several organizations or a community.
- **Flexible and Scalable:** The community cloud is flexible and scalable because it is compatible with every user. It allows the users to modify the documents as per their needs and requirement.
- **Security:** Community cloud is more secure than the public cloud but less secure than the private cloud.
- **Sharing infrastructure:** Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

Cloud Types: Community Cloud

Disadvantages of Community Cloud

- Community cloud is not a good choice for every organization.
- Slow adoption to data
- The fixed amount of data storage and bandwidth is shared among all community members.
- Community Cloud is costly than the public cloud.
- Sharing responsibilities among organizations is difficult.

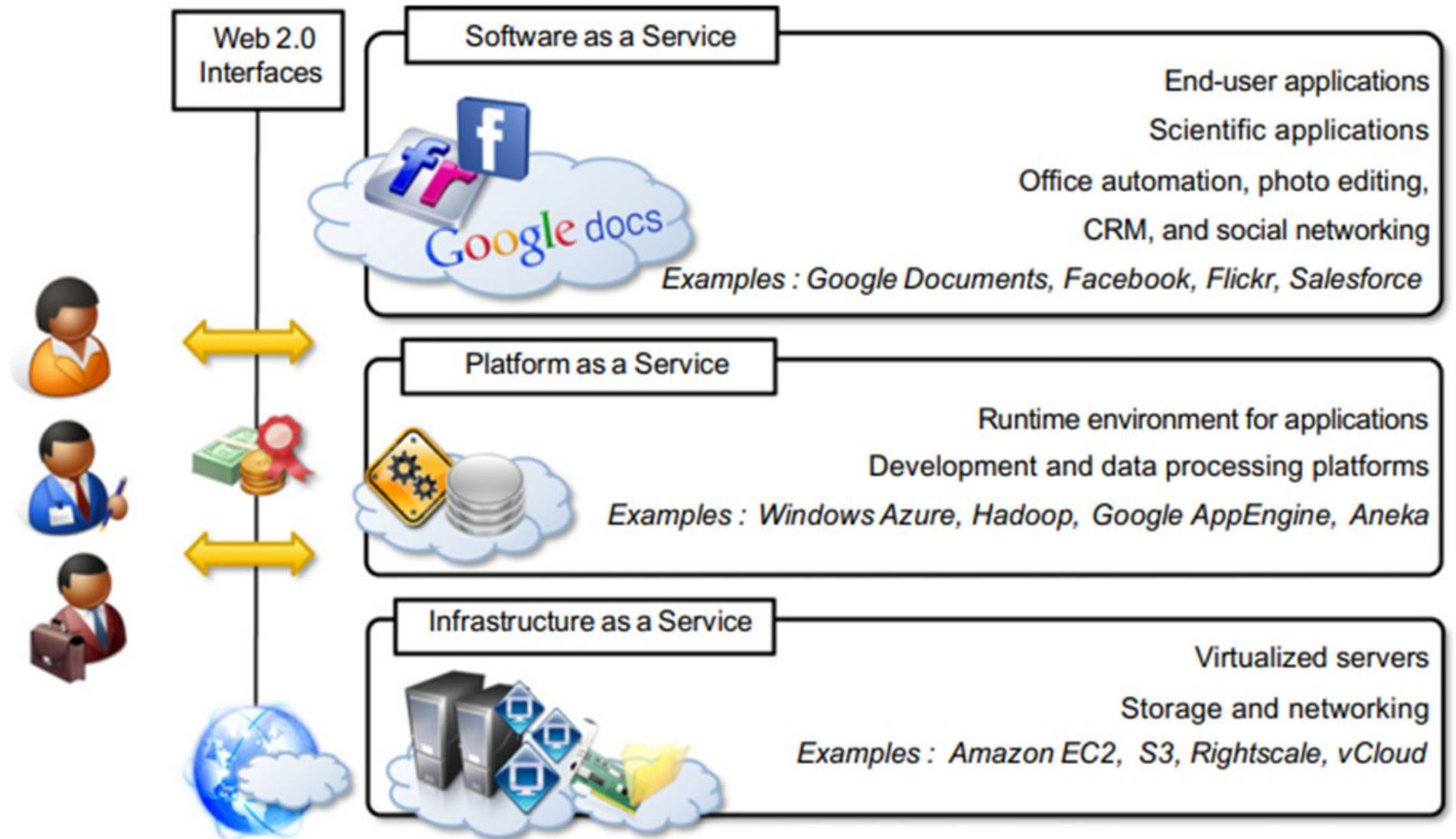
Cloud Types: Multi-Cloud

- A multi-cloud system refers to when a business uses multiple third-party cloud providers.
- Some organizations choose to use multiple cloud providers to improve their cybersecurity systems.
- Multi-cloud environments can also help maintain separate clouds for different workflows, departments or branches within their company.
- However, with a multi-cloud system, all of your cloud resources and data operate on separate infrastructures, which can make it more challenging to share resources between clouds.

Cloud Types: **High-performance computing (HPC) Cloud**

- HPC clouds specifically provide cloud services for high-performing computer applications and devices, sometimes referred to as supercomputers.
- Some organizations use supercomputers to perform complex computational tasks, such as forecasting the weather or modeling chemical molecules.
- An HPC cloud offers enough data space and server power to help ensure that supercomputers continue to run efficiently while providing organizations with the services they need.

The cloud computing reference model



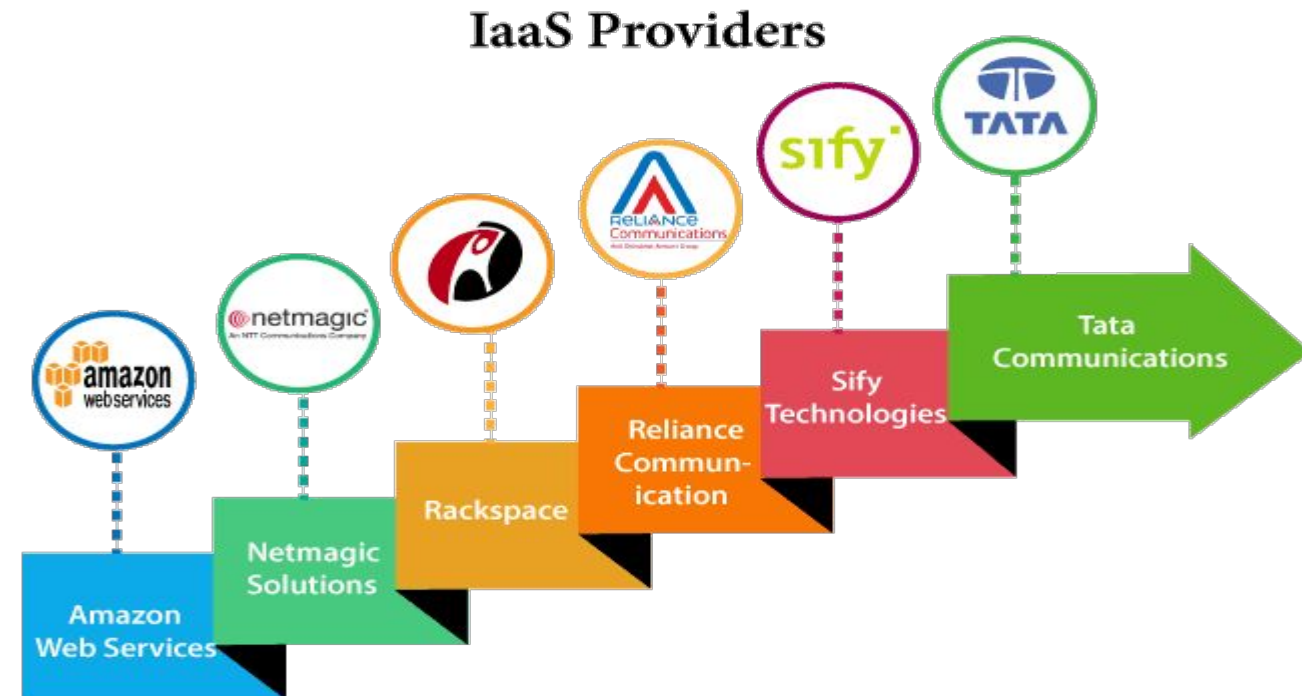
Infrastructure as a service

- IaaS is also known as **Hardware as a Service (HaaS)**
- It allows customers to **outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources**. Customers access these resources on the Internet using a **pay-as-per use model**.
- In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can **dynamically scale the configuration to meet changing requirements** and are billed only for the services actually used.
- IaaS cloud computing platform layer **eliminates the need for every organization to maintain the IT infrastructure**.
- **IaaS is offered in three models: public, private, and hybrid cloud.**
 - **The private cloud implies that the infrastructure resides at the customer-premise.**
 - **public cloud, it is located at the cloud computing platform vendor's data center**
 - **hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.**

Infrastructure as a service

IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.



Infrastructure as a service

Advantages of IaaS cloud computing layer

- 1. Shared infrastructure:** IaaS allows multiple users to share the same physical infrastructure.
- 2. Web access to the resources:** IaaS allows IT users to access resources over the internet.
- 3. Pay-as-per-use model:** IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.
- 4. Focus on the core business:** IaaS providers focus on the organization's core business rather than on IT infrastructure.
- 5. On-demand scalability:** On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Disadvantages of IaaS cloud computing layer

- 1. Security** Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.
- 2. Maintenance & Upgrade:** Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.
- 3. 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.

IaaS architecture and related components

- Compute : IaaS compute includes central processing units (CPU) inside servers for processing web requests and running applications. It also includes graphical processing units (GPU) that handle high-performance workloads and internal memory (RAM). Users can request compute resources via virtual machines, also known as virtual servers or bare metal servers.
- Virtual servers : Virtual servers are software-based servers that allow multiple virtual machines (VMs) to run simultaneously on a single "bare metal" physical server. Virtual servers rely on hypervisors that act as a layer between the physical hardware and multiple unique virtual environments. Each of these virtual environments can run its own operating system (such as Microsoft Windows, Linux® or Ubuntu).
-

IaaS architecture and related components

- Bare metal servers : Bare metal servers as a cloud service are physical machines dedicated to one single tenant who gets complete control over the physical machine. Bare metal as a service (BMaaS) features allows the user to choose their operating system, avoid the noisy neighbor challenges of shared cloud computing infrastructure, and finely tune hardware and software for specific—often data-intensive—workloads. While a traditional bare metal server does not come with a preinstalled hypervisor, this software layer can be added to virtualize the server for optimal performance.
- Networking: IaaS relies on software-defined networking (SDN), in which APIs make network hardware (for example, routers, switches, firewalls and load balancers) available. IaaS models virtualize the networking functions of this hardware, and clients can access IaaS services from anywhere over the public internet or by using a virtual private network (VPN).
- Storage : IaaS offers three types of cloud storage [i.e.](#) Block storage, File storage, Object storage

IaaS architecture and related components

- **Containers:** IaaS includes support for containerization, which packages software code with just the operating system (OS) libraries and dependencies that are required to run the code to create a single lightweight executable—a container—that runs consistently on any infrastructure. More portable and resource-efficient than virtual machines, containers have become the de facto compute units of modern cloud-native applications. In many instances, containers replaced VMs as the standard unit of process or service deployment. Container orchestration tools such as Kubernetes automate the deployment, scaling and management of containerized applications. IaaS models provide the underlying resources to scale Kubernetes and containerized applications up or down as business needs dictate.
- **IaaS security:** Third-party cloud service providers adhere to cloud security and compliance frameworks through a shared responsibility model. In essence, the cloud service provider manages the physical security of data centers (cameras, security staff) and underlying infrastructure (compute, storage, physical network).

IaaS architecture and related components

- **Development and testing:** IaaS provides an ideal testing and development environment that users can set up faster than on-premises. This feature offers DevOps and other teams the flexibility to scale dev/test environments up or down quickly, allowing organizations to bring new apps to market faster.
- **Backup and disaster recovery:** IaaS provides cloud-based backup and disaster recovery solutions, allowing organizations to replicate and back up their systems and data in the cloud. For instance, organizations can duplicate applications across multiple servers. If one server fails, another takes over, helping ensure business continuity.
- **Website hosting:** IaaS provides a cost-efficient way to host customer-facing websites and web applications that are secure, scalable and can be tailored to optimize user experiences.
- **Big data analytics:** Driven by cutting-edge technologies such as artificial intelligence (AI) and the Internet of Things (IoT), big data analytics involves the use of advanced analytic techniques against extensive, diverse big data. IaaS supports the enormous processing power needed to analyze vast amounts of data and deliver the best insights.
- **High-performance computing (HPC):** Compared to a traditional on-premises infrastructure setup, IaaS provides an efficient and cost-effective way to support high-performance computing (HPC). HPC uses supercomputers and computer clusters to solve advanced computation problems that support advances in human knowledge and create significant competitive advantages (for example, DNA sequencing, stock trading automation).
- **Hybrid multicloud adoption:** A hybrid cloud approach combines and unifies public cloud, private cloud and on-premises infrastructure to create a single, flexible, cost-optimal IT infrastructure. Today, hybrid cloud is combined with a multicloud approach, which allows companies to select best-in-class cloud services from multiple cloud vendors and avoid vendor lock-in.

Infrastructure as a service

IaaS Vendor	IaaS Solution	Details
Amazon Web Services	Elastic, Elastic Compute Cloud (EC2) MapReduce, Route 53, Virtual Private Cloud, etc.	The cloud computing platform pioneer, Amazon offers auto scaling, cloud monitoring, and load balancing features as part of its portfolio.
Netmagic Solutions	Netmagic IaaS Cloud	Netmagic runs from data centers in Mumbai, Chennai, and Bangalore, and a virtual data center in the United States. Plans are underway to extend services to West Asia.
Rackspace	Cloud servers, cloud files, cloud sites, etc.	The cloud computing platform vendor focuses primarily on enterprise-level hosting services.
Reliance Communications	Reliance Internet Data Center	RIDC supports both traditional hosting and cloud services, with data centers in Mumbai, Bangalore, Hyderabad, and Chennai. The cloud services offered by RIDC include IaaS and SaaS.
Sify Technologies	Sify IaaS	Sify's cloud computing platform is powered by HP's converged infrastructure. The vendor offers all three types of cloud services: IaaS, PaaS, and SaaS.
Tata Communications	InstaCompute	InstaCompute is Tata Communications' IaaS offering. InstaCompute data centers are located in Hyderabad and Singapore, with operations in both countries.

Platform as a service

Platform as a Service (PaaS) provides a **runtime environment**.

It allows programmers to **easily create, test, run, and deploy web applications**.

You can purchase these applications from a cloud service provider on a **pay-as-per use basis** and access them using the Internet connection.

In PaaS, back end scalability is managed by the cloud service provider, so end-users do not need to worry about managing the infrastructure.

PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.

Example: Google App Engine, Force.com, Joyent, Azure.

How does PaaS work?

PaaS simplifies app development by abstracting infrastructure complexities, allowing developers to focus on building and innovating. Here's how PaaS works:

- **Provisioning.** The cloud provider sets up the necessary computing resources, including servers, networking, and storage. They also set up a development environment that includes essential tools, frameworks, and databases.
- **Application development.** Developers write and test code using built-in development tools, SDKs, and APIs.
- **Deployment and hosting.** Developers deploy applications directly to the cloud with minimal configuration. The platform handles runtime, middleware, and operating system management.
- **Scalability and load balancing.** A PaaS automatically scales resources based on demand. Load balancing ensures efficient distribution of traffic to prevent crashes.
- **Database and storage management.** PaaS provides managed databases with backup and recovery features. It also offers scalable storage solutions for handling application data.
- **Security and maintenance.** The PaaS provider handles security patches, updates, and infrastructure maintenance. Some platforms also include built-in authentication, authorization, and encryption features.
- **Monitoring and analytics.** Tools for monitoring app performance, debugging, and logging allow developers to analyze usage patterns and optimize the application.

Platform as a service

PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools: Platform as a Service

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

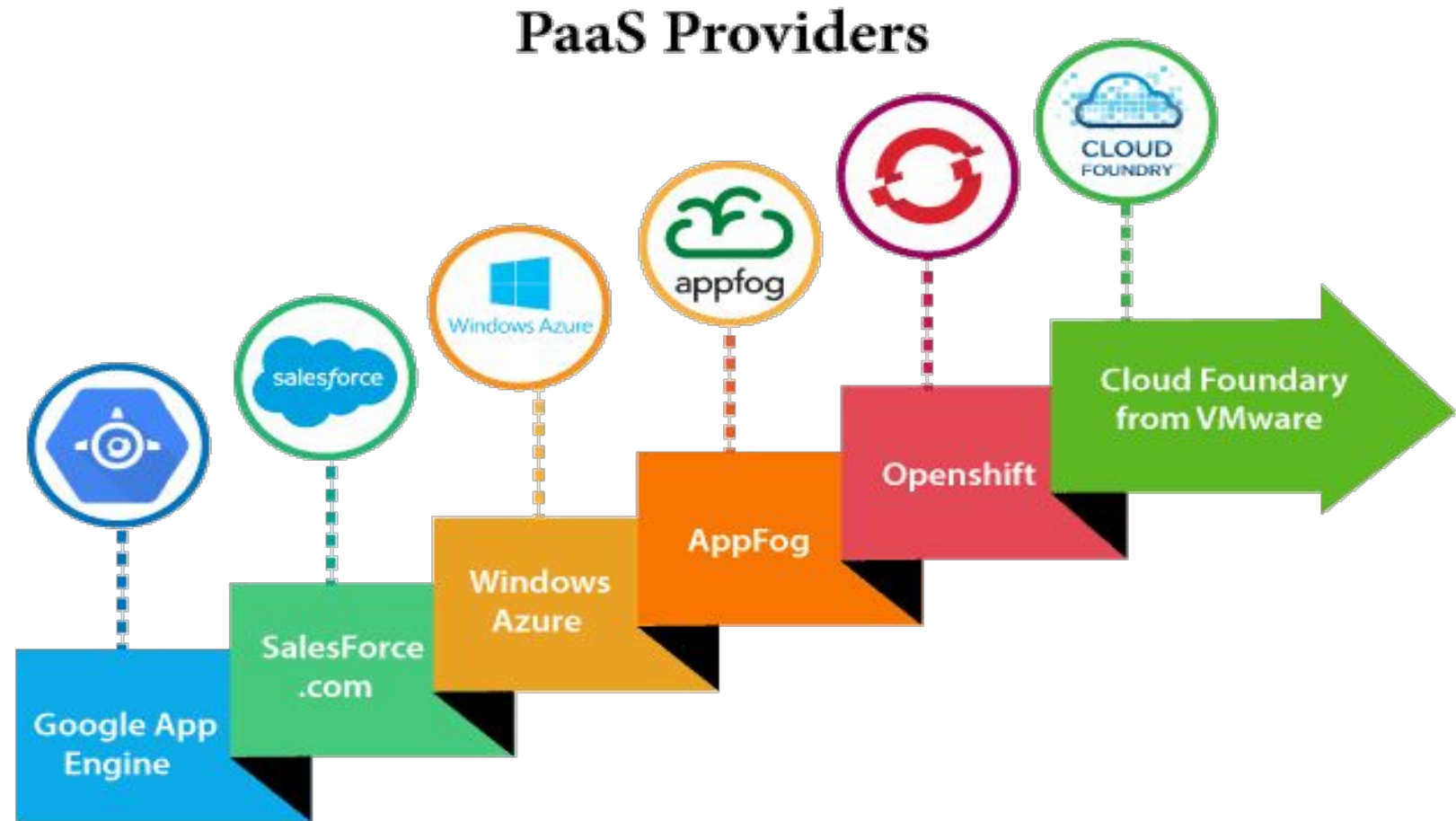
Advantages of Platform as a service

- 1) Simplified Development: PaaS allows developers to focus on development and innovation without worrying about infrastructure management.
- 2) Lower risk: No need for up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.
- 3) 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.
- 4) Instant community: PaaS vendors frequently provide online communities where the developer can get the ideas to share experiences and seek advice from others.
- 5) Scalability: Applications deployed can scale from one to thousands of users without any changes to the applications.

Disadvantages of Platform as a service

- 1) Vendor lock-in: One has to write the applications according to the platform provided by the PaaS vendor, so the migration of an application to another PaaS vendor would be a problem.
- 2) Data Privacy: Corporate data, whether it can be critical or not, will be private, so if it is not located within the walls of the company, there can be a risk in terms of privacy of data.
- 3) Integration with the rest of the systems applications: It may happen that some applications are local, and some are in the cloud. So there will be chances of increased complexity when we want to use data which in the cloud with the local data.

Platform as a service



Platform as a service

Providers	Services
Google App Engine (GAE)	App Identity, URL Fetch, Cloud storage client library, Logservice
Salesforce.com	Faster implementation, Rapid scalability, CRM Services, Sales cloud, Mobile connectivity, Chatter.
Windows Azure	Compute, security, IoT, Data Storage.
AppFog	Justcloud.com, SkyDrive, GoogleDocs
Openshift	RedHat, Microsoft Azure.
Cloud Foundry from VMware	Data, Messaging, and other services.

Software as a service

SaaS is also known as "**On-Demand Software**". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

There are the following services provided by SaaS providers -

Business Services - SaaS Provider provides various business services to start-up the business. 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 - As we all know, social networking sites are used by the general public, so 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.

How SaaS works

- SaaS takes advantage of cloud computing infrastructure and economies of scale to provide customers a more streamlined approach to adopting, using and paying for software.
- *SaaS applications are built to be hosted on the cloud.* SaaS software vendors can host application on their own cloud infrastructure or with a cloud service provider. Hosting with an established provider can help businesses achieve greater scalability and global accessibility.
- *SaaS applications are accessible to any customer with an internet connection and an internet-connected user device.* SaaS applications typically run in any web browser and on any computer or mobile device, but they often run more effectively on mobile phones and tablets. And in some instances, SaaS applications can offer or require a dedicated thin client, a lightweight computing device that runs remotely on resources stored on a central server.
- *SaaS applications use multi-tenant architecture,* where a single instance of a software application (and its underlying database and hardware) serves multiple tenants (or user accounts). To maintain data security and privacy, each tenant's application data, user data, system data and custom configurations are segregated from those of other customers.
- *SaaS applications require little to no management and zero maintenance from the customer.* The SaaS vendor is responsible for provisioning, managing and maintaining all the servers and infrastructure required to run the application, and for applying feature upgrades and security patches when necessary. They provide load balancing and data backup features, infrastructure redundancies, and disaster recovery services to prevent outages and meet service level agreements (SLAs).

Software as a service



Software as a service

- SaaS is also known as "**On-Demand Software**". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.
- There are the following services provided by SaaS providers -
- **Business Services** - SaaS Provider provides various business services to start-up the business. 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** - As we all know, social networking sites are used by the general public, so 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.

Software as a service- Advantages

- SaaS is easy to buy: SaaS pricing is based on a monthly fee or annual fee subscription, so it allows organizations to access business functionality at a low cost, which is less than licensed applications. SaaS providers are generally pricing the applications using a subscription fee
- 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: The software is hosted remotely, so 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. The initial set-up cost for SaaS is typically less than the enterprise software. SaaS vendors are pricing their applications based on some usage parameters, such as a number of users using the application. So SaaS does easy to monitor and automatic updates.
- 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. SaaS reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.
- Multidevice support: SaaS services can be accessed from any device such as desktops, laptops, tablets, phones, and thin clients.
- 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.

Software as a service

Disadvantages of SaaS cloud computing layer

- Security: Actually, data is stored in the cloud, so security may be an issue for some users. However, cloud computing is not more secure than in-house deployment.
- Latency issue: Since data and applications are stored in the cloud at a variable distance from the end-user, there is a possibility that there may be greater latency when interacting with the application compared to local deployment. Therefore, the SaaS model is not suitable for applications whose demand response time is in milliseconds.
- 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 also.

Software as a service

Provider	Services
Salseforce.com	On-demand CRM solutions
Microsoft Office 365	Online office suite
Google Apps	Gmail, Google Calendar, Docs, and sites
NetSuite	ERP, accounting, order management, CRM, Professionals Services Automation (PSA), and e-commerce applications.
GoToMeeting	Online meeting and video-conferencing software
Constant Contact	E-mail marketing, online survey, and event marketing
Oracle CRM	CRM applications
Workday, Inc	Human capital management, payroll, and financial management.

Xaas

"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.

benefits of XaaS

- **Expenditure model improvements.** With XaaS, businesses can cut costs by purchasing services from providers on a subscription basis. Before XaaS and cloud services, businesses had to buy separate products-software, hardware, servers, security, infrastructure-install them on-site, and then link everything together to form a network. With XaaS, businesses buy what they need and pay on the go. The previous capital expenditure now becomes an operating expense.
- **Speed up new apps and business processes.** This model allows businesses to adopt new apps or solutions to changing market conditions. Using multi-tenant approaches, cloud services can provide much-needed flexibility. Resource pooling and rapid elasticity support mean that business leaders can add or subtract services. When users need innovative resources, a company can use new technologies, automatically scaling up the infrastructure.
- **Transferring IT resources to high-value projects.** Increasingly, IT organizations are turning to a XaaS delivery model to streamline operations and free up resources for innovation. They are also harnessing the benefits of XaaS to transform digitally and become more agile. XaaS gives more users access to cutting-edge technology, democratizing innovation. In a recent survey by Deloitte, 71% of companies report that XaaS now constitutes more than half of their company's enterprise IT.

Benefits in XaaS :

Cost Saving – When an organization uses XaaS then it helps in cost-cutting and simplifies IT deployments.

Scalability –XaaS can easily handle the growing amount of work by providing the required resources/service.

Accessibility – It helps in easy accessing and improving accessibility as long as the internet connection is there.

Faster Implementation –It provides faster implementation time to various activities of the organization.

Quick Modification – It provides updates for modification as well as undergoes quick updating by providing quality services.

Better Security –It contains improved security controls and is configured to the exact requirements of the business.

Boost innovation – While XaaS is used it Streamlines the operations and frees up resources for innovation.

Flexibility – XaaS provides flexibility by using cloud services and multiple advanced approaches.

disadvantages of Xaas

- **Possible downtime.** The Internet sometimes breaks down, and when this happens, your XaaS provider can be a problem too. With XaaS, there can be issues of Internet reliability, flexibility, provisioning, and management of infrastructure resources. If XaaS servers go down, users will not be able to use them. XaaS providers can guarantee services through SLAs.
- **Performance issues.** As XaaS becomes more popular, bandwidth, latency, data storage, and recovery times can be affected. If too many clients use the same resources, the system may slow down. Apps running in virtualized environments can also be affected. Integration issues can occur in these complex environments, including the ongoing management and security of multiple cloud services.
- **Complexity effect.** Advancing technology for XaaS can relieve IT workers from day-to-day operational headaches; however, it can be difficult to troubleshoot if something goes wrong.
- Internal IT staff still needs to stay updated on new technology. The cost of maintaining a high-performance, a robust network can add up - although the overall cost savings of the XaaS model are usually enormous. Nonetheless, some companies want to maintain visibility into their XaaS service provider's environment and infrastructure. Furthermore, a XaaS provider that gets acquired shuts down a service or changes its roadmap can profoundly impact XaaS users.

Benefits in XaaS :

Disadvantages in XaaS :

Internet Breakage – Internet breaks sometimes for XaaS service providers where there can also be issues in internet reliability, provisioning, and managing the infrastructure resources.

Slowdown –When too many clients are using the same resources at the same time, the system can slow down.

Difficult in Troubleshoot – XaaS can be a solution for IT staff in day-to-day operational headaches, but if anywhere problem occurs it is harder to troubleshoot it as in XaaS multiple services are included with various technologies and tools.

Change brings problems –If a XaaS provider discontinues a service or alters it gives an impact on XaaS users.

XaaS is on the rise now :

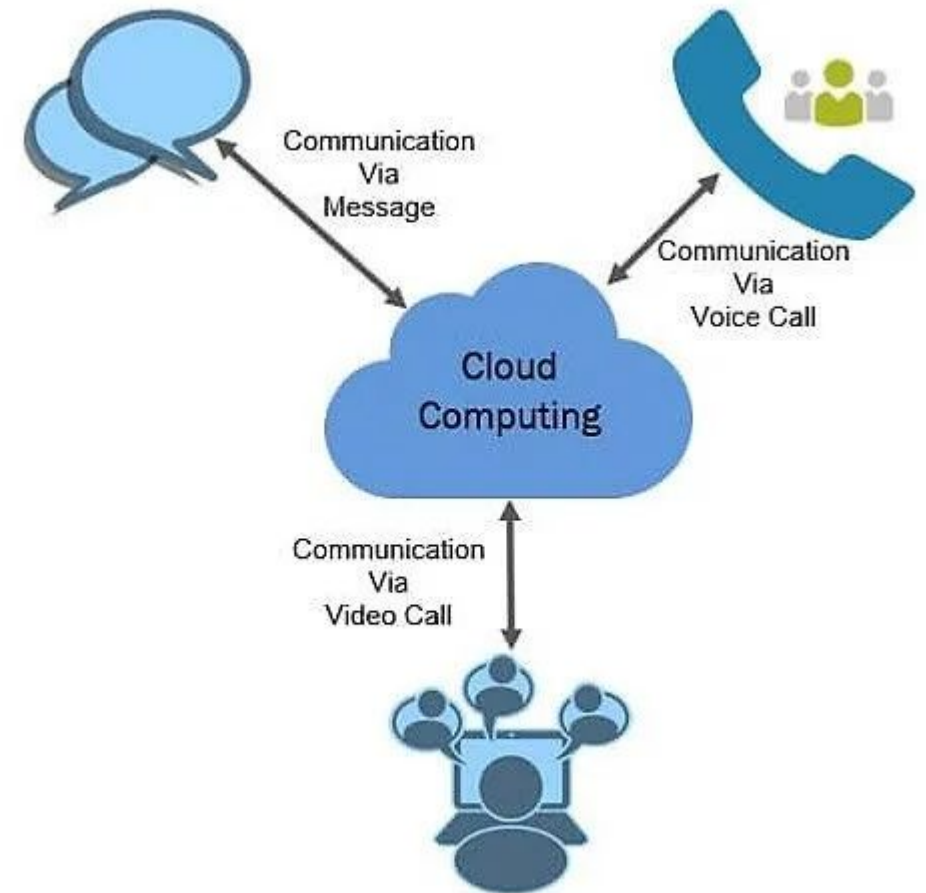
Public cloud services are growing at an exponential rate. Researchers assumed that global cloud computing revenue is going to reach \$342 billion dollars by 2025. Through the XaaS model by servitization, products and services are combined through which businesses innovate faster and enhance their relationship with customers which further increases their revenue.

Future of XaaS :

A combination of cloud computing and good internet access allows accessing good quality XaaS services and better improvement of XaaS. Some companies are not confident to take XaaS because of security and business governance concerns. But service providers increasingly reveal these concerns which allow organizations which put additional workloads into the cloud.

Xaas: Communication as a Service (CaaS)

This model comprises solutions for different communication like IM, VoIP, and video conferencing applications which are hosted in the provider's cloud. Such a method is cost-effective and reduces time expenses.



Xaas: Communication as a Service (CaaS)

Common CaaS Services

- **Voice over IP (VoIP):** Internet-based telephone services for voice calls.
- **Instant Messaging (IM):** Text-based communication services.
- **Video Conferencing:** Services for conducting video calls and meetings.
- **Unified Communications:** Bundled solutions that integrate various communication channels into a single platform.
- **Contact Center Automation:** Tools like Interactive Voice Response (IVR), Automatic Call Distribution (ACD), and automated dialing.
- **Outbound Notifications:** Services to automate high-volume communications, such as appointment reminders.

Advantages of Communication as a Service (CaaS)

- By eliminating customers from investing in the infrastructure and Software necessary for communication services, CaaS offers an affordable option to give communication services to their customers.
- The CaaS vendor offers its clients round-the-clock support.
- Customers who use a CaaS vendor's services are not required to spend money or time administering the CaaS components.
- CaaS vendors provide flexible services because they bill on a pay-as-you-go basis.
- They deliver services in response to consumer demand, CaaS offers scalable services.
- CaaS offers a hosted and managed solution that only has one vendor manage all aspects of communication.
- Since the vendors are in charge of updating the carrier platform, there is no danger of the service becoming dated from the client's standpoint.

Drawbacks of CaaS

- One potential drawback of CaaS is the loss of control over the quality of service. While providers of CaaS typically offer high-quality service levels, there is always the potential for problems to arise. Businesses may not have many options if there are problems with service quality besides changing suppliers.
- Another potential drawback is the cost of CaaS. While the upfront costs may be lower than traditional communication solutions, the ongoing costs can add up over time. Businesses should consider the total ownership cost before signing up for a CaaS solution.
- Finally, businesses should know that CaaS solutions are hosted in the cloud. This means that businesses will need to have reliable Internet access to use the service. If there are any problems with the Internet connection, the CaaS solution will not be available.

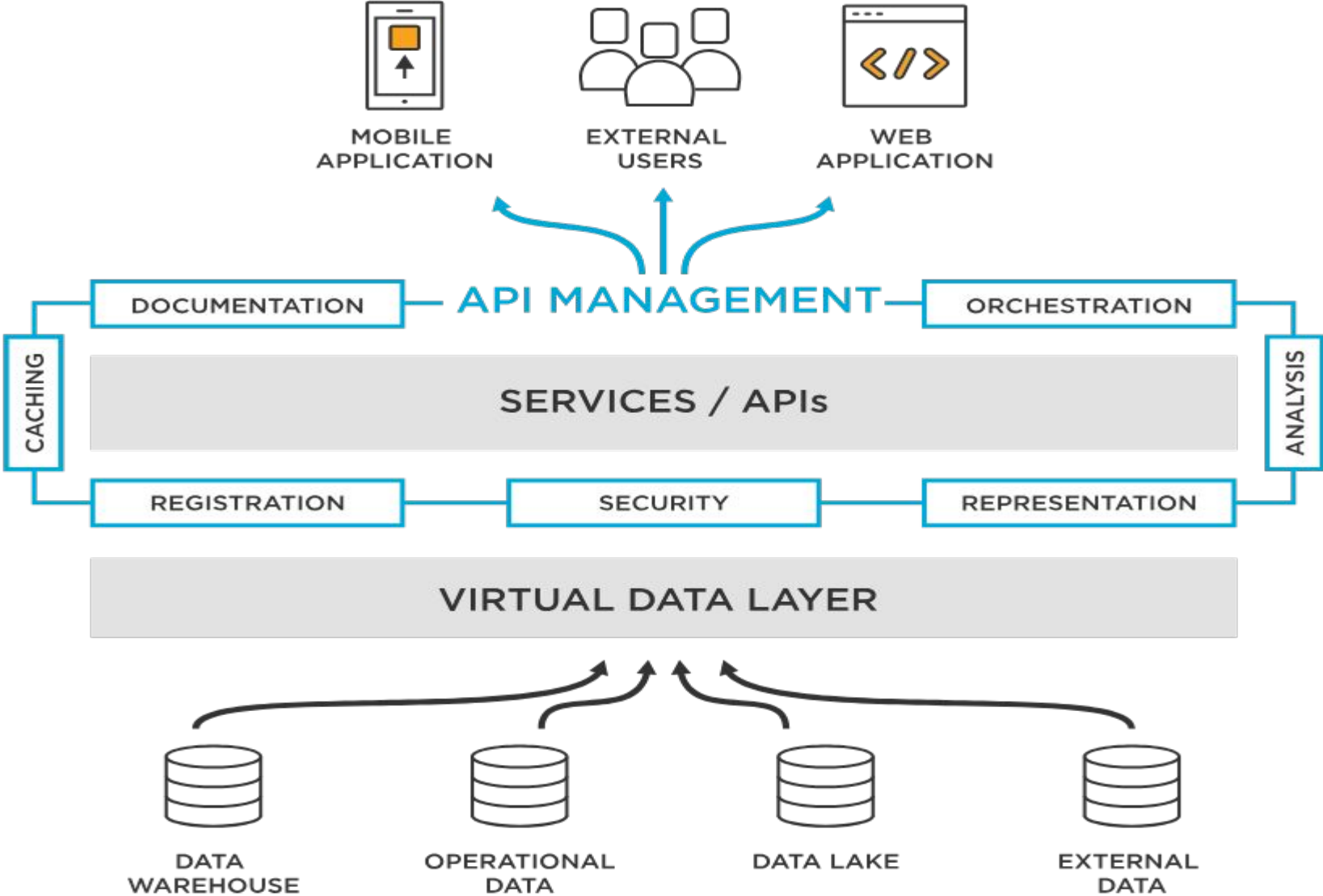
CAAS

<https://www.youtube.com/watch?v=4j8uP-sp5Jo&t=144s>

Xaas: Desktop as a Service (DaaS) –

- DaaS provider mainly manages storing, security, and backing up user data for desktop apps. And a client can also work on PCs using third-party servers.
- Desktop as a service (DaaS) is defined as a cloud-based service where vendors stream desktops, operating systems, and application images remotely to users' devices and look after provisioning, maintenance, upgrades, and other routine tasks, all through a one-stop-shop subscription offering.
- DaaS not only provides the benefits of virtualization but also saves on the cost and effort of hosting virtual desktops in privately owned mainframes and servers.

DaaS Providing Full Abstraction for Virtual Desktops



How DaaS works

- **Backend management:** The DaaS provider hosts the virtual desktop infrastructure (VDI), including the servers, storage, network resources, and virtual machines (VMs).
- **Access:** End users connect to their virtual desktop via a secure application or web browser on devices such as a laptop, tablet, thin client, or smartphone.
- **Authentication:** Users log in with secure credentials to access their virtual desktop environment, which is provisioned for them.
- **Security:** All data is stored in the cloud, rather than on the user's local device. This ensures that sensitive information is not compromised if a device is lost or stolen.
- **Streaming:** The DaaS provider streams the virtual desktop environment, along with applications and data, to the user's device. This allows access to powerful software, even on lower-powered hardware.

DAAS

<https://www.youtube.com/watch?v=lvFFa57dCsA>

the disadvantages of DaaS.

- **It requires a high-speed connection to the internet** – While internet access is increasingly easy to obtain or find in public, DaaS might not be ideal for employees who work in very remote areas that don't have internet coverage.
- **It could cost more over time** – While DaaS costs less than VDI when it comes to CapEx, the monthly subscription costs could, over time, add up to be more than the initial cost of VDI.
- **There's a learning curve** – Employees need to be trained to access virtual desktops through a web browser or a specialized application, and that can be a roadblock to widespread adoption.
- **It can be tough to estimate needs** – Depending on the DaaS platform, organizations might not know exactly how much memory or computing power the virtual desktops should have.
- **Risk of software licensing issues** – If an organization has software licenses for applications installed on on-premises workstations, those licenses don't always apply to virtual desktops – so there could be some extra costs there.
- **Fewer customization options** – DaaS can't match the level of customizability that VDI offers, since VDI is built in-house to an organization's specifications.

Benefits of DaaS

- **Gain the best of both worlds** – DaaS provides the centralization, security, and ease of management of virtual desktop infrastructure (VDI) and the simplicity and convenience of a managed service.
- **Eliminate the need for capital expenditures (CapEx) or specialized IT skills** – The DaaS hardware is owned and managed by the provider so organizations don't have to provide or manage dedicated PCs or other equipment.
- **Scale simply and efficiently** – Because it's fast and easy to spin up new virtual desktops as needed, organizations can efficiently handle scalability as they add new employees or scale back after a specific desktop-intensive project.
- **Pay only for what you use** – The subscription model makes DaaS cost-effective and doesn't require large up-front costs.
- **Enhance customer experiences** – With employees' ability to work and respond to customers from wherever they are, organizations can stay accessible and responsive.
- **Streamline budgeting** – Because each desktop comes with a fee, it's easy to predict and control desktop costs. With in-office desktop workstations, costs can be unpredictable because you don't know when a machine will break down or need maintenance.
- **Reduce security risks** – If an employee's device is lost or stolen, their desktop and applications aren't accessible to the thief because they're stored in the cloud and only accessible via that user's login credentials.

Is DaaS the same as virtual desktop infrastructure?

- The answer is no; virtualization is a part of DaaS, but desktop as a service includes several
- other cloud-delivered services priced on a subscription model.
- Virtual desktop infrastructure (VDI) solutions such as DaaS offerings deliver desktops to devices from a consolidated data center. This is why the two terms are commonly confused. However, the infrastructure underpinning the VDI solution is typically on-premise and controlled by the IT department.
- A cloud provider administers the storage, computation, and network infrastructure in the DaaS model. The organization offering desktops to its staff can oversee the desktop operating system, apps, anti-virus software, and any other desktop-related tasks or even partner with a managed desktop service provider.
- DaaS eliminates the substantial upfront costs that come with establishing VDI on-premise. Typically, DaaS offerings come with a subscription-based plan that requires no upfront payment. Additionally, you can delegate all the administrative tasks necessary to support, repair, adapt, or update the VDI.

Types of DAAS

- **Persistent:** Users can personalize and retain a desktop to look identical every time they sign in. However, persistent desktops need more storage space than non-persistent desktops, making them more costly.
- **Non-persistent:** When a user signs out, their desktop gets wiped clean. It is just a means of accessing cloud-based shared resources.

Xaas Security as a Service (SECaaS) –

In this method, the provider integrates security services with the company's infrastructure through the internet which includes anti-virus software, authentication, encryption, etc.

- Continuous monitoring of every threat by SECaaS
- Security analysts handle cyber security
- Proactive threat management helps to detect malfunctions proactively which could lead to compromise
- Sophisticated techniques are deployed to detect intrusions
- Automated response to SPAM and virus and its elimination

Working of SECaaS:

When the IT department installs virus protection software, [spam](#) filtering software, and other security tools on every computer, on the network, or on the server in your geographic location, keeping the package up to date or instructing them to use it, security solutions are no longer delivered regionally with security as a service

The former method of doing things involved paying direct pricing for hardware as well as ongoing fees for licenses to allow for the usage of that security code, which made it much more expensive. Instead, security as a service makes it simple and rational to use similar technologies.

Security can be availed by the following alliances:

Encryption: makes the data unreadable until it has been authentically decoded, or encrypted.

Network security: Network access management protocols are used to secure and keep an eye on network services.

Email security: Protects against email frauds, spam, phishing, malware etc.

Identification: Users can access with a valid log-in ID and legal permission, else forbids if it is not authenticated.

Data loss prevention: Tools are built to monitor and secure data to protect from data loss.

Benefits of SECaaS

- Greater security for the enterprises
- Latest version of security tools and software's available for enterprise security
- Company can hire qualified security personnel to enhance organization and support organization security posture
- Faster delivery of security related services
- No new hardware and license to be renewed instead it may be upgraded or replaced with new version as required on lesser costs
- Log management outsourcing helps to save time for focus on core skills

Challenges of SECaaS

- **Legacy hardware elimination thought migration** – overestimation of cloud security outsourcing advantages are tough to assess as you may be left susceptible during transition period switching from legacy security to cloud based security.
- **Risks of misconfiguration** – Configuration errors lead to cloud security breaches. There might be issues if there is a provisioning error by an internal team or cloud provider.
- **Accountability** – Managed security provider and client share jointly responsibility of security breach. Enterprises need to reduce risks of outsourcing by implementation and enforcement of rules to address vulnerabilities in cloud related to security.

Identity management as a Service

- Identity-as-a-service, or IDaaS, is an application delivery model (like software-as-a-service, or SaaS) that allows users to connect to and use identity management services from the cloud.
- Also referred to as cloud-based identity security, the shift to deploy IDaaS began several years ago and was led by companies with a digitally driven IT adoption strategy.
- Many IDaaS systems leverage the power of cloud computing and adaptive authentication as a way of improving or speeding up these business processes. This level of IAM computing uses online computer power, database storage, and other IT resources.
- Identity management ensures the right people in an organization have the right access to the right resources.
- Using IDaaS technology to properly identify, authenticate, and authorize employees within an organization, these systems use access rights to prevent unauthorized users gaining access to confidential files or documents.
- With cybersecurity threats continuing to grow, identity and access management helps keep your protection organized.

Definition of an Identity –

- An identity refers to a set of attributes or characteristics which make something recognizable or known. It is digital identity of an individual that is mostly concerned in computer network systems. An attribute and metadata of any object related to another object that enables an object to be identifiable is termed as Digital Identity. An identity can belong to an individual and may consist of the following:
- Things you are: Biological characteristics like gender, age etc.
- Things you know: Personal data like social security PINs etc.
- Things you have: Your fingerprint, bank account which you can access etc.
- Things you relate to: Your family and friends, beliefs and values etc.
- Example: Multi-factor authentication (MFA): MFA is the use of multiple authentication factors to verify a user's identity.
- One example would be **requiring users to insert a USB device into their laptop, in addition to entering their password.**

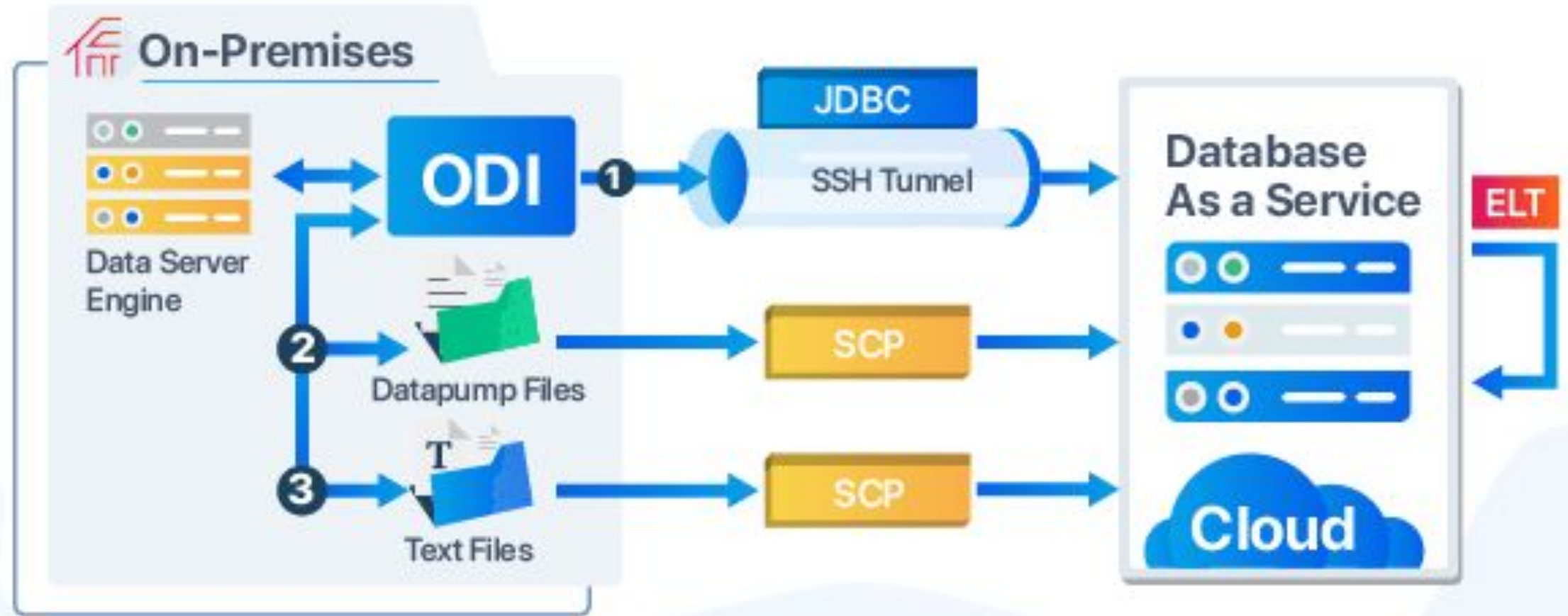
IDaaS providers can offer a number of user authentication services, such as:

- Multi-factor authentication (MFA): MFA is the use of multiple authentication factors to verify a user's identity. One example would be requiring users to insert a USB device into their laptop, in addition to entering their password. MFA is more secure than username and password combinations alone. Cloud MFA providers enable organizations to quickly implement MFA. (See also: What is two-factor authentication?)
- Single sign-on (SSO): SSO allows users to sign in once to a single portal in order to access all of their SaaS applications, and it also provides a centralized place for companies to manage the applications each user has access to. Most SSO services are cloud-hosted and allow users to access their SSO login pages through a web browser.
- Identity management: An identity provider (IdP) stores and manages user identities. An IdP may check user identities via username-password combinations and other factors, or it may simply provide a list of user identities that another service provider checks. Cloud-hosted IdPs fit under the IDaaS umbrella.

Database as a Service

- Database as a service (DBaaS) is a cloud computing managed service offering that provides access to a database without requiring the setup of physical hardware, the installation of software or the need to configure the database.
- Most database administration and maintenance tasks are handled by the service provider, enabling users to quickly benefit from the database service.
- The use of DBaaS is growing as more organizations shift from on-premises systems to cloud databases. DBaaS vendors include cloud platform providers that sell database software and other database makers that host their software on one or more of the cloud platforms.
- Most DBaaS environments run on public cloud infrastructure, but some cloud providers will also install their DBaaS technologies in on-premises data centers and manage them remotely for customers in private clouds or hybrid cloud infrastructures.
- under the DBaaS model, the provider maintains the system infrastructure and database and delivers it as a fully managed cloud service. The service covers high-level administrative functions, such as database installation, configuration, maintenance and upgrades. Additional tasks, such as backups, patching and performance management, typically are also handled by the provider.
- Example: **AWS cloud with an Oracle or SQL Server database through Amazon Relational Database Service.**

Database as a Service



DBaaS Working

DBaaS providers host data and database infrastructure while enabling access through API endpoints. They offer features like alerts, notifications, monitoring, constant support, and geo-replication for backups and availability.

1. DBaaS is delivered over the internet and users can access it through a web-based interface or API.
2. It can help to reduce the complexity and cost of managing databases.
3. It allows the development team to deploy and access a database without worrying about hardware purchase, hardware setup, database installation, and configuration, database maintenance and administration.
4. The organizations can free up the resources to focus on strategic initiatives by offloading tasks like data backup, recovery, etc. to a service provider.
5. It provides disaster recovery capability and helps to improve the availability and performance of databases.

How to Choose a DBaaS?

1. **Database Type:** Determine the type of database needed. If you need a relational database like MySQL or a non-relational database like MongoDB.
2. **Performance:** Evaluate the performance capabilities such as latency, throughput before deciding the DBaaS.
3. **Uptime:** Check provider's Service Level Agreement to check for uptime guarantees.
4. **Security:** Check to ensure that DBaaS offers robust security features like data encryption, Identity and Access Management, and network security.
5. **Cost:** Consider the cost related to storage, data transfer, understand the pricing model and ensure that it aligns with your budget.
6. **Documentation:** Look for comprehensive and detailed documentation to help with setup and troubleshooting.

Benefits of DBaaS

1. **Scalability:** DBaaS can automatically scale resources up and down based on the demand, ensuring cost-efficiency and optimal performance.
2. **High Availability:** DBaaS services ensures high availability as they often include built-in redundancy and failover mechanisms.
3. **Reliability:** DBaaS services ensures high reliability and business continuity with automated backup and disaster recovery solutions to help protect data against loss.
4. **Cost-efficiency:** DBaaS services offer pay-as-you-go pricing that allow organizations to pay only for the resources they use.
5. **Performance Optimization:** DBaaS providers ensures consistent performance by managing and optimizing the underlying infrastructure.
6. **Flexibility:** Many DBaaS providers support a variety of database engines like SQL, NoSQL, thus giving organizations the flexibility to choose the best tool for their needs.

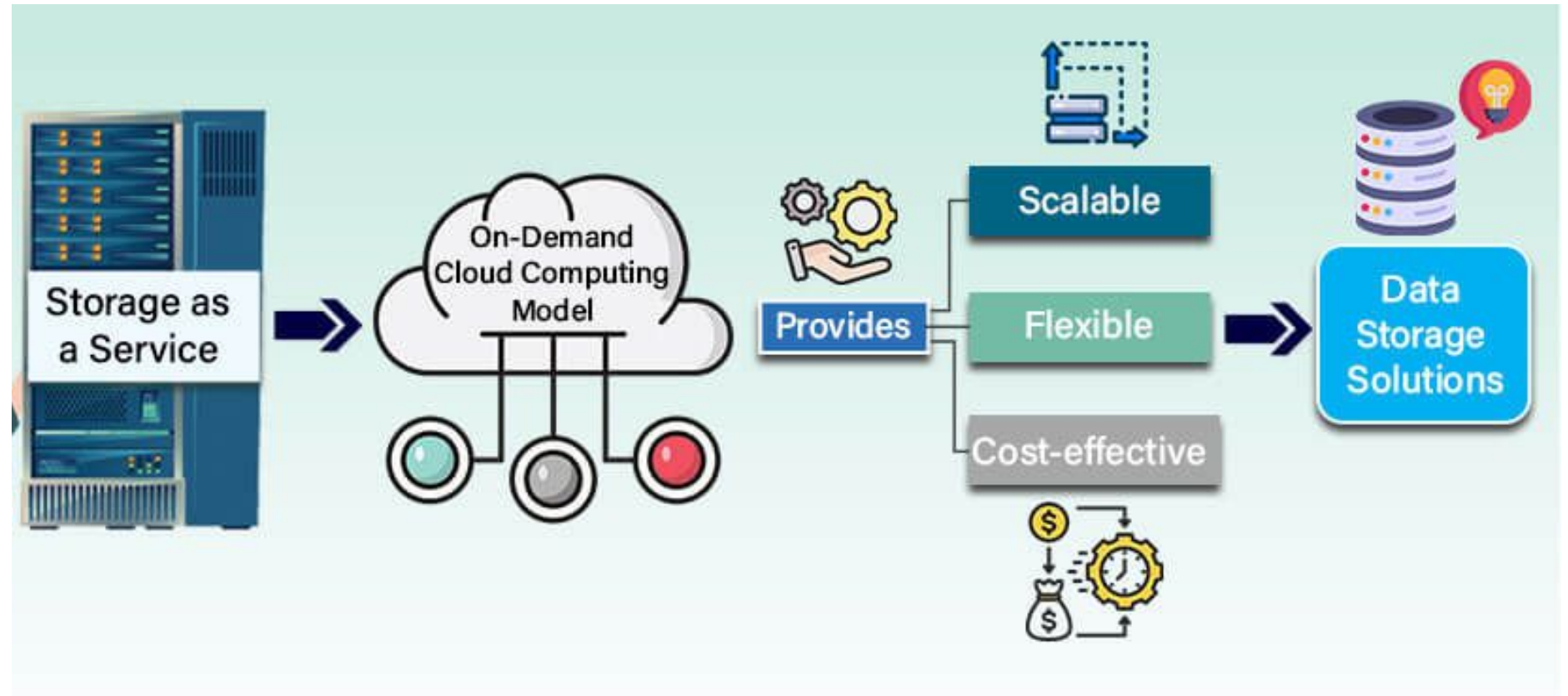
Limitations of DBaaS

1. **Performance Variability:** DBaaS operates on shared resources due to which sometimes performance can vary due to resource contention with other tenants.
2. **Complex Customizations:** Sometimes it can be difficult to optimize the database for specific needs as users have limited control over the underlying hardware and software.
3. **Hidden Costs:** Additional storage charges and charges for premium features can lead to unexpected expenses.
4. **Complex Data Portability:** Transferring huge volumes of data between providers or back to on-premises systems can be complex and costly.
5. **Time-consuming Data Transfer:** Migrating large datasets to a DBaaS platform can be time-consuming and may require downtime.

Storage as a Service

- Storage as a Service (STaaS) is the practice of using public cloud storage resources to store your data. Using STaaS is more cost efficient than building private storage infrastructure, especially when you can match data types to cloud storage offerings.
- Storage as a Service or STaaS is cloud storage that you rent from a Cloud Service Provider (CSP) and that provides basic ways to access that storage.
- Enterprises, small and medium businesses, home offices, and individuals can use the cloud for multimedia storage, data repositories, data backup and recovery, and disaster recovery.
- There are also higher-tier managed services that build on top of STaaS, such as Database as a Service, in which you can write data into tables that are hosted through CSP resources.
- The key benefit to STaaS is that you are offloading the cost and effort to manage data storage infrastructure and technology to a third-party CSP
- Examples of STaaS vendors include **Dell EMC, Hewlett Packard Enterprise (HPE), NetApp and IBM.**

Storage as a Service



Types of Cloud Storage

Block-based storage system: This type of storage system organizes data into fixed-sized blocks, which are typically accessed at a low level by the operating system or applications

- It resembles cloud-based hard drives.
- It involves volume partitioning and formatting.
- Provides direct access to drives, volumes and partitions.

File-based storage system: Unlike block-based systems, file-based storage systems organize data into files and folders.

- Utilize Network-Attached Storage (NAS) devices.
- Facilitates file sharing over the network.
- Simplifies storage access over the network.

Objective-based storage system: This type of storage system treats data as objects rather than files or blocks.

- Utilizes HTTP protocols and REST APIs for data operations.
- Prioritizes simplicity and accessibility.
- Offers a flat structure for objects and files.

STaaS benefits

- Cut infrastructure costs
- Simplify scaling
- Retain flexibility
- Strengthen and preserve data
- Reduce latency
- Encourage transformation

Advantages of STaaS

- Accessibility from anywhere with an internet connection.
- Scalability to meet changing data storage needs.
- Cost-effectiveness with pay-as-you-go pricing.
- Data redundancy and high reliability.
- Automatic backup and recovery features.
- Easy collaboration and file sharing.

Disadvantages of STaaS

- Dependency on internet connection.
- In some cases data access may be slower as compare to on-premises storage.
- Integrating STaaS with existing IT infrastructure and applications can be complex.
- Users have limited control over the storage infrastrucutre in STaaS.

Xaas

Healthcare as a Service (HaaS) –

The healthcare industry has opted for the model HaaS service through electronic medical records (EMR). IoT and other technologies have enhanced medical services like online consultations, health monitoring 24/7, medical service at the doorstep e.g. lab sample collection from home, etc.

Transport as a Service (TaaS) –

Nowadays, there are numerous apps that help in mobility and transport in modern society. The model is both convenient and ecological friendly e.g. Uber taxi services is planning to test flying taxis and self-driving planes in the future.

Collaboration as a Service

- Enterprise customers increasingly depend on a mixture of voice, video, messaging, customer care, web conferencing, and telepresence services to collaborate internally and keep in touch with their customer bases. The diversity of these collaborative channels means that customers' IT professionals need to be expert with many different technology solutions. These solutions are always changing and getting better, with more services and richer capabilities. All of this adds up to significant CapEx and OpEx spend.
- Cloud collaboration is a **type of enterprise collaboration that allows employees to work together on documents and other data types, which are stored off-premises and outside of the company firewall**. Employees use a cloud-based collaboration platform to share, edit and work together on projects.
- Example : Applications like **Cisco Webex, Microsoft Teams, Skype and Zoom** enable video conferencing, instant messaging and document sharing. Cloud storage. Tools for document storage, such as Dropbox, Google Docs and WeTransfer, let users share files as well as store and edit them in real time.

Working of Collaboration as a service

1. Cloud-Based Platforms:

Instead of local servers, files and applications are hosted on remote cloud servers.

2. Centralized Document Storage:

Documents and data are stored in a single, central location, creating a "single source of truth" for the team.

3. Real-Time Co-Authoring:

Multiple team members can open and edit the same file at the same time.

4. Synchronization:

All changes are saved and synced automatically, so everyone sees the most current version of the document.

5. Access from Anywhere:

Users can access and contribute to projects from any device with an internet connection, supporting flexibility and remote work.

Benefits

- **Real-Time Collaboration:** Fosters immediate teamwork and reduces project delays.
- **Eliminates Version Control Issues:** Prevents confusion caused by multiple conflicting document versions.
- **Improved Accessibility:** Allows employees to access shared resources and data from any location.
- **Enhanced Productivity:** Streamlines workflows and simplifies complex tasks through integrated tools and automated processes.
- **Flexibility for Remote Teams:** Supports distributed workforces, enabling seamless collaboration across different geographical locations.

Examples of CaaS Platforms

- **Google Docs:** Enables real-time editing and sharing of documents.
- **Microsoft Teams:** A platform for communication, file sharing, and project collaboration.
- **Slack:** A messaging and collaboration tool for teams.
- **Zoom & Google Meet:** Tools for real-time video conferencing, a form of collaboration.

Compliance as a Service

- A Compliance as a Service (CaaS) application would need to oblige as a third party. CaaS may require to be architecture as its own layer of a Service Oriented Architecture (SOA) in order to be reliable. A CaaS may be needed to be able to manage cloud relationships, comprehend security rules and procedures, know how to operate data and administer privacy, deliver an incidence feedback, archive, and enable the system to be queried. This is a huge order, but CaaS has the capability to be a good value-added service.
- CaaS system built inside a private cloud in which the data is under control of a single entity, thus confirming that the data is under that entity's secure control and that transaction is audited. Indeed, major cloud computing compliance systems have been created with the help of private cloud. A well-implemented CaaS service may measure the risk of servicing compliance and ensure or indemnify tenancy against that risk. CaaS can be brought to bear as mechanism to guarantee that an e-mail conformed to particular standards, anything which may be new electronic service of a network of national postal system and something which may help in ending the scourge of spam.
- The major services that should provided additionally in a Compliance as a Service (CaaS) offering:
 - Database access control
 - Separation of duties
 - Annual risk assessment
 - Application management
 - Change control
 - Data discovery
 - Data masking
 - Incident response
 - Policy creation and enforcement
 - Real-time data protection
 - Repair of vulnerabilities
 - Personnel training
 - Service configuration

- **Advantages of Compliance as a Service (CaaS) –**
- In cloud, Encryption is quite arduous to track which is simplified by the Compliance as a Service. To fulfill the needs of end user and organizations around governance including compliance, they use a cloud provider's service. These services deliver pre-built behaviors with specific regulations, such as needed encryption levels.
- Compliance as a Services are configurable i.e. no development is required. This is cost effective for the organizations and it reduce the maintenance along with changing regulations, as well as internal and external policies of the corporations.
- **Disadvantages of Compliance as a Service (CaaS) –**
- Cloud service consumers will be held responsible for any issues with the compliance services. Its mandatory that customer validate the compliance services to ensure that there are no issues.
- It is impossible to Compliance as a Service providers to support all the regulations among all the countries. Also, as all the services are cloud based then there is always a risk that providers will stop to providing the services at any time because of low uses of their services. So, end-user and organization become dependent on service providers. Overall these are some critical aspects which falls under drawbacks of CaaS.
- example: In healthcare, **the Health Insurance Portability and Accountability Act (HIPAA) requires network administrators to create logical boundaries between protected and unprotected workflows.** In finance, the Sarbanes-Oxley Act (SOX) requires specific encryption levels for different data types.

Monitoring as a Service

- Monitoring as a Service (MaaS) is a security service that provides security to IT assets of any business 24/7. It plays a vital role in securing an enterprise or government clients from any possible cyber threats. MaaS is a monitoring service that can be outsourced in a flexible and consumption-based subscription model.
- **Monitoring as a Service** (MaaS) provides you with the security solutions that are essential for the organizations that are reliant on the IT infrastructure. However, for effective and efficient monitoring, the organization must have up to date technology, experts knowing advanced technical skills, scalable security processes and all this come with a tremendous expense.
- If compared to the traditional security operations centre MaaS exceed in two important things:
- The total cost of ownership was higher in the traditional security operations centre.
- Traditional security operations are less effective.

Features of Monitoring as a Service

1. Protection Against External and Internal Threats: The security monitoring services analyze the alerts from security devices 24/7 in real-time. The security analyst collects data from various security devices to recognize the threats and thereby imply effective measures to respond to these threats.
 - a. Early Detection: The information security team detects and discloses the security threats as soon after they appear. The threats are reported to the customer via emails. This reports describes the vulnerabilities in the security of the system and also describes its effect on the systems or application. The report may also include the protective measures that you can take for these vulnerabilities.
 - b. Dashboard Interface: The dashboard interface is implemented as a platform, control and service monitoring. This conceptualizes your system and its resource at one place and eases the information security team to monitor the operation status of the platform being monitor. The information security team try to find the reason of vulnerability by navigating back in time and visualize how the system was performing before the problem occurred and how it is performing after the problem has occurred. As the root cause of the vulnerability is understood the preventive measure are suggested to resolve the issue.
 - c. Log Centralization and Analysis: It is a monitoring solution which involves the correlation of log entries and matching of the log entries. Analyzing this correlation and matching of log entries set a benchmark for the operational performance and provide an index of the security threats. An alarm is raised if an incident moves above the benchmark parameters. This alarm or warning is analyzed by security experts responsible for the quick response for such threat incidents.

Features of Monitoring as a Service

- d. Vulnerabilities Detection and Management: This service provides periodic automated testing which exposes the threat to information system over the internet. The service identifies threats such as unauthorized access to the administrative services, the services that have not been updated for a long.
- e. Continuous System Patching/Upgrade and Fortification: The level of security is enhanced with the continuous system patching. System patching is nothing but enhancing the computer program to fix the vulnerabilities and bugs in the computer program. System patching is very important as it not only raises the security level of your system but also supports the newer version of the application and software installed on your system.
- f. Intervention, Forensics, and Help Desk Services: We all are familiar with the help desk that provides you with quick assistance to your problems. Similarly, the MaaS vendor has a team of experts with ample of knowledge that intervenes whenever any threat is detected. They provide 24/7 assistance to support and maintain the applications and infrastructure. Whenever a threat is detected it requires the forensic analysis to check out how much time cost and effort it will require to fix it.

Features of Monitoring as a Service

2. Delivering Business Values: Most of the customer consider build-vs-buy decision is better if compared to calculating return on investment (ROI). But when calculated it is observed that cost of building a security monitoring infrastructure along with the security monitoring team is more as compared to the outsourcing a MaaS service provider. The MaaS vendors have a complete information security infrastructure along with a team of skill and the expert individual who are updated with the latest technology. The MaaS vendors provide the scalable services which is an advantage for their customers. If the company try and built its own security infrastructure it must have to focus on the staff attrition, technical updates, scheduling operations, identifying the vulnerabilities and also find the solution to resolve them. Outsourcing the MaaS services eliminates all these headaches. Well if you want to evaluate the loss incurred by the external or internal incident the parameters that you must take into account are the amount of loss occurred, frequency of loss incurred and estimate the probability of occurring the loss. This is not an actual method to calculate the loss incurred but it helps you in tracking the security metric. While outsourcing any service you must consider and quantify the risk involved in it. It will raise your confidence that your investment will succeed. A scalable service is more valuable as the customers can get additional business benefit by giving some additional cost.

3. Real-Time Log Monitoring Enables Compliance: Log monitoring is a process of recording log messages into a file which helps the developers or administrator to understand how the system or application is being used. Real-time log monitoring helps in quick detection of errors, failed process and services. It also provides alerts for network and protocol failures. It warns the developers of infrastructure problems. MaaS provides automation for this time-consuming process.

Monitoring as a Service

Advantages of MaaS

- MaaS provide a ready to use a monitoring tool to its customer at a very minimal price.
- MaaS leverage the customer to focus on their business instead of worrying about the information security of their enterprise.
- MaaS provides 24/7 assistance to its customers, who can report the issues and get immediate assistance from the MaaS team.

- Example : CloudManix tool

Network as a Service

- Network-as-a-service (NaaS) is a cloud service model in which customers rent networking services from cloud providers. NaaS allows customers to operate their own networks without maintaining their own networking infrastructure. Like other cloud services, NaaS vendors run networking functions using software, essentially allowing companies to set up their own networks entirely without hardware. All they need is Internet connectivity.
- NaaS can replace virtual private networks (VPNs), multiprotocol label switching (MPLS) connections, or other legacy network configurations. It can also replace on-premise networking hardware such as firewall appliances and load balancers. A newer model for routing traffic and applying security policies, NaaS has had a major impact on enterprise networking architecture.

Advantages of NaaS

- **Flexibility:** Cloud services offer more flexibility and greater customization. Changes are made to the network via software, not hardware. IT teams are often able to reconfigure their corporate networks on demand.
- **Scalability:** Cloud services like NaaS are naturally more scalable than traditional, hardware-based services. Enterprise NaaS customers can simply purchase more capacity from a vendor instead of purchasing, plugging in, and turning on more hardware.
- **Access from anywhere:** Depending on how a cloud-based network is configured, users may be able to access it from anywhere — and on any device — without using a VPN, although this introduces the need for strong access control. Ideally, all a user needs is an Internet connection and login credentials.
- **No maintenance:** The cloud provider maintains the network, managing software and hardware upgrades.
- **Bundled with security:** NaaS makes it possible for a single provider to offer both networking services and security services like firewalls. This results in tighter integration between the network and network security.
- **Cost savings:** This advantage depends on the vendor. However, purchasing cloud services instead of building one's own services often results in cost savings: cloud customers do not need to purchase and maintain hardware, and the vendor already has the servers they need to provide the service.
- **Advantages:** NaaS services can range from **managed software-defined WAN (SD-WAN) and network access including wireless to security, unified communications services, and more**—either in a public cloud or on virtualized customer premise equipment (vCPE).

Function as a Service

- FaaS is a type of cloud computing service. It provides a platform for its users or customers to develop, compute, run and deploy the code or entire application as functions. It allows the user to entirely develop the code and update it at any time without worrying about the maintenance of the underlying infrastructure. The developed code can be executed with response to the specific event. It is also **as same as PaaS**.
- FaaS is an event-driven execution model. It is implemented in the serverless container. When the application is developed completely, the user will now trigger the event to execute the code. Now, the triggered event makes response and activates the servers to execute it. The servers are nothing but the Linux servers or any other servers which is managed by the vendor completely. Customer does not have clue about any servers which is why they do not need to maintain the server hence it is **serverless architecture**.
- Both PaaS and FaaS are providing the same functionality but there is still some differentiation in terms of Scalability and Cost.
- FaaS, provides auto-scaling up and scaling down depending upon the demand. PaaS also provides scalability but here users have to configure the scaling parameter depending upon the demand.
- In FaaS, users only have to pay for the number of execution time happened. In PaaS, users have to pay for the amount based on pay-as-you-go price regardless of how much or less they use
- Example : data processing (e.g., batch processing, stream processing, extract-transform-load (ETL)), Internet of things (IoT) services for Internet-connected devices, mobile applications, and web applications.

Function as a Service

Advantages of FaaS :

- **Highly Scalable:** Auto scaling is done by the provider depending upon the demand.
- **Cost-Effective:** Pay only for the number of events executed.
- **Code Simplification:** FaaS allows the users to upload the entire application all at once. It allows you to write code for independent functions or similar to those functions.
- Maintenance of code is enough and no need to worry about the servers.
- Functions can be written in any programming language.
- Less control over the system.
- The various companies providing Function as a Service are Amazon Web Services – Firecracker, Google – Kubernetes, Oracle – Fn, Apache OpenWhisk – IBM, OpenFaaS,

Xaas

Hardware as a Service (HaaS) –

Managed Service Providers (MSP) provide and install some hardware on the customer's site on demand. The customer uses the hardware according to service level agreements. This model is very similar to IaaS as computing resources present at MSP's site are provided to users substituted for physical hardware.

Network as a Service

- Network-as-a-service (NaaS) is a cloud service model in which customers rent networking services from cloud providers. NaaS allows customers to operate their own networks without maintaining their own networking infrastructure. Like other cloud services, NaaS vendors run networking functions using software, essentially allowing companies to set up their own networks entirely without hardware. All they need is Internet connectivity.
- NaaS can replace virtual private networks (VPNs), multiprotocol label switching (MPLS) connections, or other legacy network configurations. It can also replace on-premise networking hardware such as firewall appliances and load balancers. A newer model for routing traffic and applying security policies, NaaS has had a major impact on enterprise networking architecture.

Advantages of NaaS

- **Flexibility:** Cloud services offer more flexibility and greater customization. Changes are made to the network via software, not hardware. IT teams are often able to reconfigure their corporate networks on demand.
- **Scalability:** Cloud services like NaaS are naturally more scalable than traditional, hardware-based services. Enterprise NaaS customers can simply purchase more capacity from a vendor instead of purchasing, plugging in, and turning on more hardware.
- **Access from anywhere:** Depending on how a cloud-based network is configured, users may be able to access it from anywhere — and on any device — without using a VPN, although this introduces the need for strong access control. Ideally, all a user needs is an Internet connection and login credentials.
- **No maintenance:** The cloud provider maintains the network, managing software and hardware upgrades.
- **Bundled with security:** NaaS makes it possible for a single provider to offer both networking services and security services like firewalls. This results in tighter integration between the network and network security.
- **Cost savings:** This advantage depends on the vendor. However, purchasing cloud services instead of building one's own services often results in cost savings: cloud customers do not need to purchase and maintain hardware, and the vendor already has the servers they need to provide the service.
- **Advantages:** NaaS services can range from **managed software-defined WAN (SD-WAN) and network access including wireless to security, unified communications services, and more**—either in a public cloud or on virtualized customer premise equipment (vCPE).

