

# CLOUD COMPUTING, SECURITY AND PRIVACY

—

## Course Objectives:

- This course will enable students to:
  - Discuss the concepts, characteristics, delivery models and benefits of cloud computing.
  - Explore the key technical, organisational and compliance challenges of cloud computing.
  - Explore the security issues that arise from cloud computing architectures intended for delivering Cloud based enterprise IT services.

## MODULE - I

**Introduction:** The Evolution of Cloud Computing; **What Is Cloud Computing?:** Cloud Computing Defined, The SPI Framework for Cloud Computing, The Traditional Software Model, The Cloud Services Delivery Model, Cloud Deployment Models, Key Drivers to Adopting the Cloud, The Impact of Cloud Computing on Users, Governance in the Cloud, Barriers to Cloud Computing Adoption in the Enterprise.

**8 Hours**

## MODULE - II

**Infrastructure Security:** Infrastructure Security: The Network Level, Infrastructure Security: The Host Level, Infrastructure Security: The Application Level.

**Data Security and Storage:** Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.

**8 Hours**

### MODULE - III

**Identity and Access Management:** Trust Boundaries and IAM, Why IAM?, IAM Challenges, IAM Definitions, IAM Architecture and Practice, Relevant IAM Standards and Protocols for Cloud Services, IAM Standards, Protocols, and Specifications for Consumers, Comparison of Enterprise and Consumer Authentication Standards and Protocols, IAM Practices in the Cloud, Cloud Authorization Management, Cloud Service Provider IAM Practice

**8 Hours**

### MODULE - IV

**Security Management in the Cloud:** Introduction, Security Management Standards, Security Management in the Cloud, Availability Management, SaaS Availability Management, PaaS Availability Management, IaaS Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

**8 Hours**

### MODULE - V

**Privacy:** What Is Privacy?, What Is the Data Life Cycle?, What Are the Key Privacy Concerns in the Cloud?, Who Is Responsible for Protecting Privacy? Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing, Legal and Regulatory Implications, U.S. Laws and Regulations, International Laws and Regulations.

**Audit and Compliance:** Internal Policy Compliance, Governance, Risk, and Compliance (GRC), Illustrative Control Objectives for Cloud Computing, Incremental CSP-Specific Control Objectives, Additional Key Management Control Objectives, Control Considerations for CSP Users, Regulatory/External Compliance, Other Requirements, Cloud Security Alliance, Auditing the Cloud for Compliance.

**8 Hours**

# Cloud Computing

Cloud computing is the delivery of computing resources **over the internet, or "the cloud", on a pay-as-you-go basis.**

Standard definition of cloud computing is based on five attributes:

**multitenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources.**



## Multitenancy (shared resources)

Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), **Cloud computing is based on a business model in which resources are shared** (i.e., multiple users use the same resource) at the **network level, host level, and application level.**

- **Traditional (previous) computing models**
- In the past, computing was often **resource-dedicated**.
- Example:
  - A company bought its own servers.
  - Those servers were used **only by that company**.
  - All the processing power, storage, and applications were **reserved** for them.
- **Drawback:** Expensive to buy and maintain, often underutilized because the capacity wasn't always fully used.

# Massive scalability

Although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.

## 1. Traditional limitations

- Even large organizations with **hundreds or thousands of servers** have a physical limit.
- Expanding means **buying, installing, and configuring** more hardware — which takes time, money, and physical space.

## 2. Cloud computing advantage

- Cloud providers like AWS, Azure, or Google Cloud have **huge data centers** with vast amounts of computing power, storage, and network bandwidth.
- They can give you access to **tens of thousands of virtual systems** almost instantly.
- You can also expand **network bandwidth** and **storage space** on demand without worrying about the underlying hardware.

## **Pay as you go**

Users pay for only the resources they actually use and for only the time they require them.

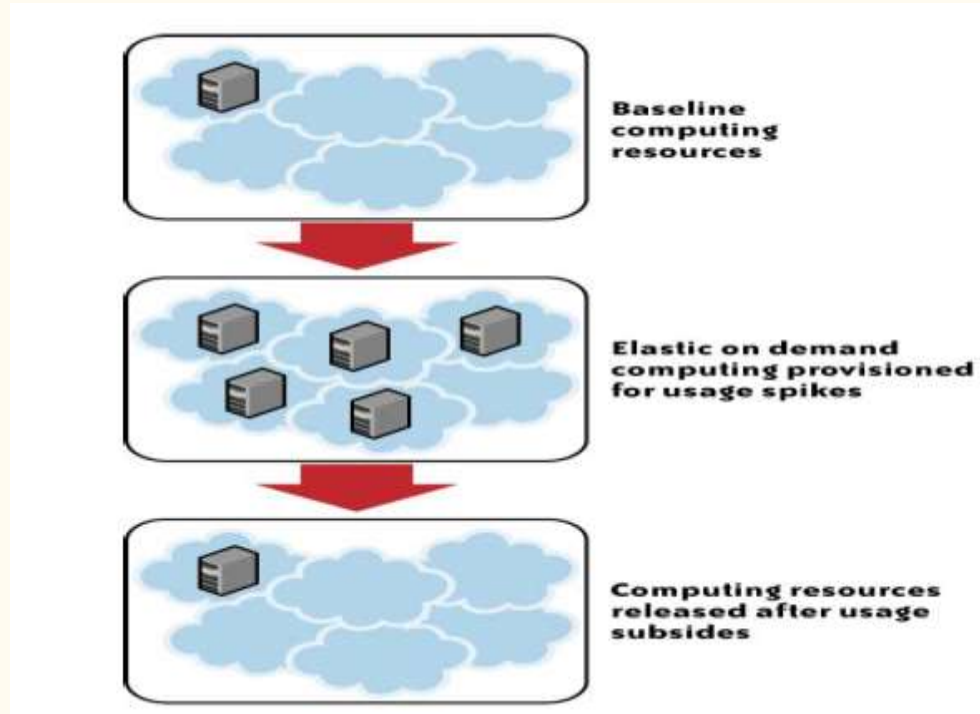
## **Self-provisioning of resources**

Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

# Elasticity

- One of the attributes of cloud computing is **elasticity of resources**. This cloud capability allows users to increase and decrease their computing resources as needed,
- There is always an awareness of the baseline of computing resources, but predicting future needs is difficult, especially **when demands are constantly changing**.
- Cloud computing can offer a means to provide IT resources on demand and address spikes in usage.

# Fig: Attribute of Elasticity



## 1. Baseline computing resources

- **What it means:** Your normal or everyday resource usage.
- **Example:**
  - A company usually needs only 1 server to handle its regular website traffic.
  - This is the **minimum steady-state capacity** that stays available all the time.

## 2. Elastic on-demand computing (usage spikes)

- **What it means:** When demand suddenly increases (e.g., a sale, product launch, or seasonal rush), the cloud **automatically provisions extra computing resources**.
- **How it works:**
  - Virtual machines, storage, or bandwidth are added instantly.
  - The business doesn't need to physically install new hardware.
- **Example:**
  - An online store's traffic jumps from 500 to 5,000 users per minute during a flash sale — the cloud spins up 4 extra servers to handle the load.

### 3. Resources released after usage subsides

- **What it means:** Once demand drops back to normal, the extra resources are **deallocated**.
- **Benefit:**
  - You stop paying for the extra capacity.
  - Prevents waste of unused computing power.
- **Example:**
  - After the sale ends, traffic returns to normal — the cloud shuts down the extra 4 servers and returns to the baseline 1 server.

## Recent notable cloud launches

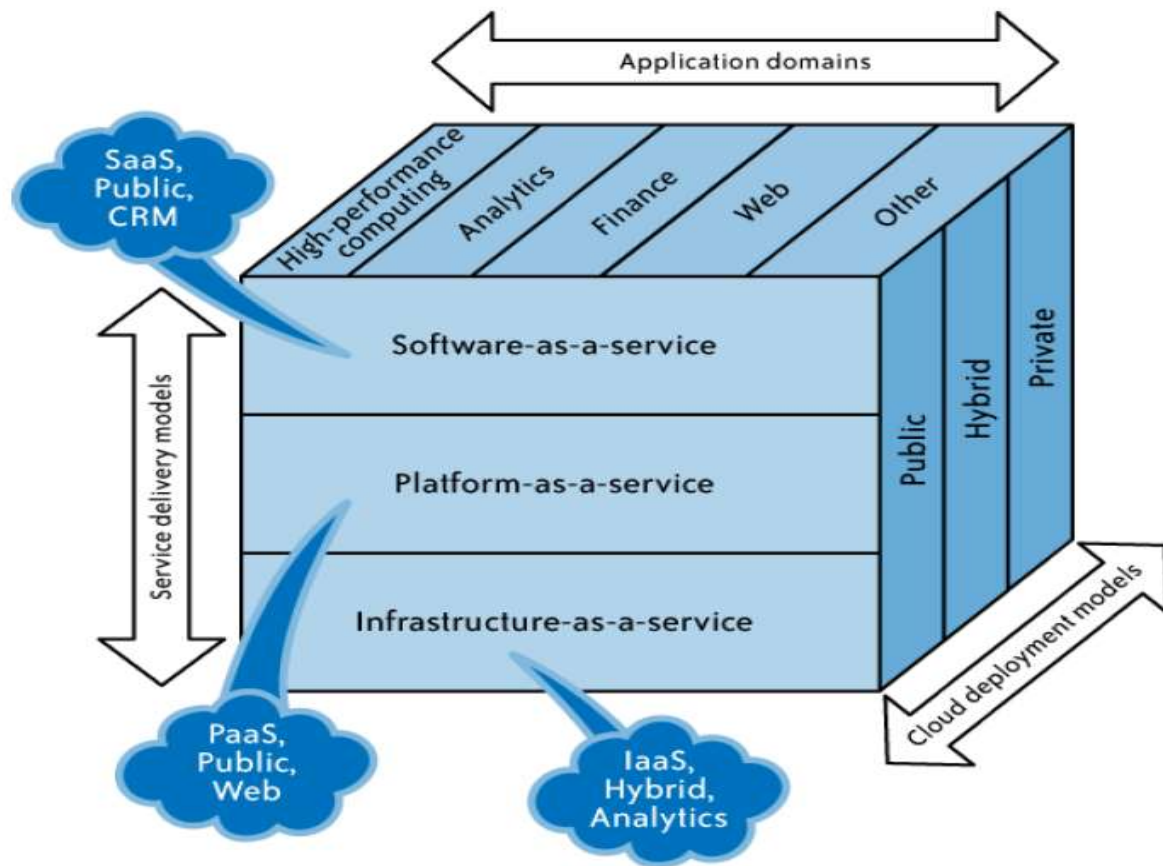
Cloud applications	Desktop and business applications
	 
Cloud software development platform	Software platform to host cloud-based enterprise applications
	 Windows Azure   <small>Success. Not Software.</small>
Cloud-based infrastructure	Servers, storage, security, databases
	   

# The SPI Framework for Cloud Computing

A commonly agreed upon framework for describing cloud computing services goes by the acronym “SPI.” This acronym stands for the three major services provided through the cloud:

**software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service(IaaS).**

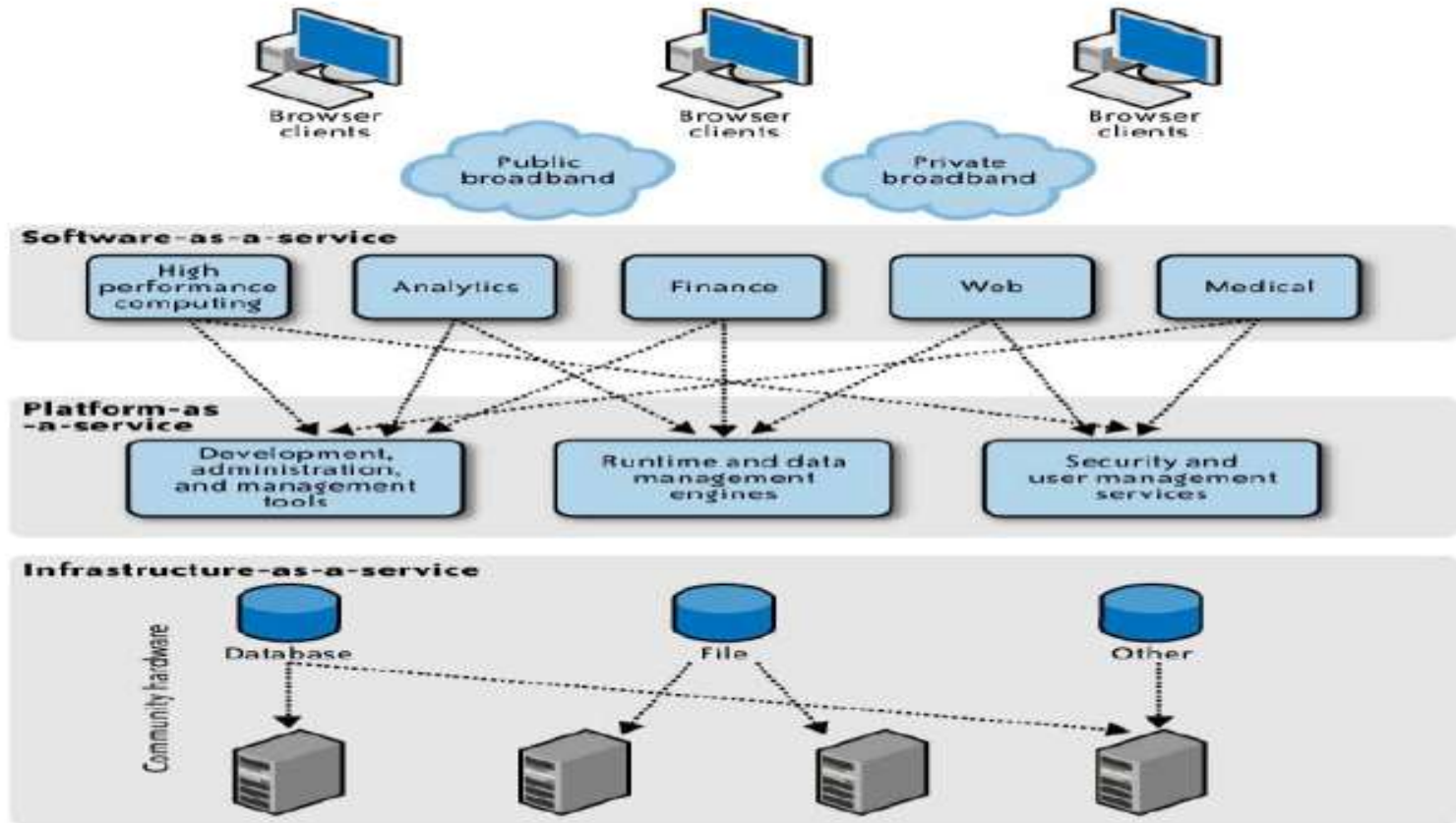
**Figure illustrates the relationship between services, uses, and types of clouds.**



# Relevant Technologies in Cloud Computing

- Cloud computing isn't so much a technology as it is the **combination of many pre existing** technologies.
- These technologies have matured at different rates and in different contexts, and were not designed as a coherent whole; however, they have come together to create a technical ecosystem for cloud computing.
- New advances in **processors, virtualization technology, disk storage, broadband Internet connection, and fast, inexpensive servers** have combined to make the cloud a more compelling solution.

# Architecture for relevant technologies



## 1. Browser Clients & Connectivity

- **Users** (browser clients) connect to cloud services via:
  - **Public broadband** (e.g., the Internet)
  - **Private broadband** (e.g., corporate network/VPN)

## 2. Software-as-a-Service (SaaS) — *Top Layer*

- SaaS delivers complete applications over the internet.
- Users don't manage infrastructure or platforms — they just use the application.
- **Examples shown in the diagram:**
  - **High performance computing** (e.g., simulations, scientific calculations)
  - **Analytics** (e.g., BI tools)
  - **Finance** (e.g., online banking, ERP finance modules)
  - **Web** (e.g., website hosting, CMS)
  - **Medical** (e.g., telemedicine platforms)

### 3. Platform-as-a-Service (PaaS) — *Middle Layer*

- Provides tools and environments to build, test, and deploy applications.
- **Examples in the diagram:**
  - Development, administration, and management tools
  - Runtime and data management engines (to execute code and manage data)
  - Security and user management services

### 4. Infrastructure-as-a-Service (IaaS) — *Bottom Layer*

- Delivers the basic building blocks: servers, storage, and networking.
- **Examples in the diagram:**
  - Database storage
  - File storage
  - Other infrastructure resources
- These are **community hardware** resources hosted by cloud providers.

## **Cloud access devices**

The range of access devices for the cloud has expanded in recent years.

Home PCs, enterprise PCs, network computers, mobile phone devices, custom handheld devices, and custom static devices (including refrigerators) are all online.

## Browsers and thin clients

- Users of multiple device types can now access applications and information from wherever they can load a browser.
- Indeed, browsers are becoming increasingly sophisticated.
- Enterprise applications, such as SAP and Oracle, can be accessed through a browser interface—a change from when a client (a so-called “fat”) application needed to be loaded onto the desktop.

**High-speed broadband access :** A critical component of the cloud is the broadband network, which offers the means to connect components and provides one of the substantial differences from the utility computing concept of 30 years ago.

**Data centers and server farms** Cloud-based services require large computing capacity and are hosted in data centers and server farms. These distributed data centers and server farms span multiple locations and can be linked via internetworks providing distributed computing and service delivery capabilities.

**Storage devices** Decreasing storage costs and the flexibility with which storage can be deployed have changed the storage landscape. The fixed direct access storage device (DASD) has been replaced with storage area networks (SANs), which have reduced costs and allowed a great deal more flexibility in enterprise storage.

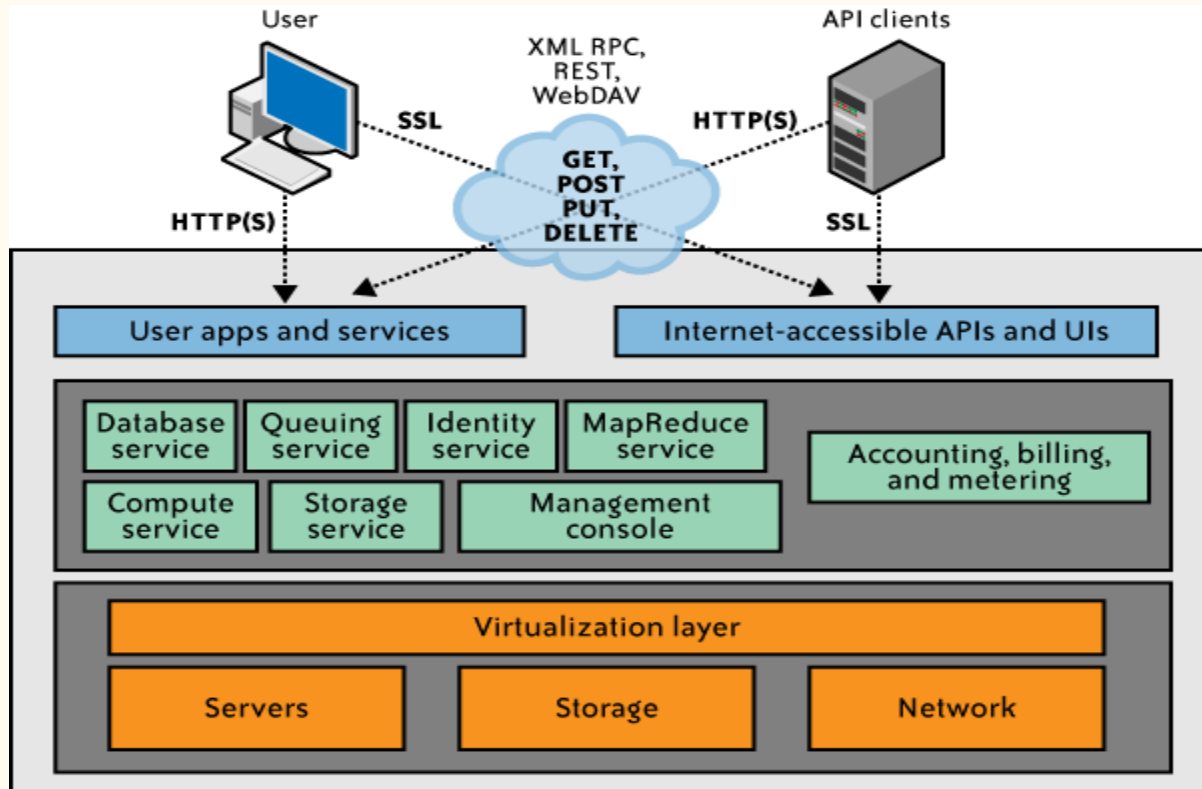
SAN software manages integration of storage devices and can independently allocate storage space on demand across a number of devices.

- A **SAN** is a **high-speed, specialized network** that connects storage devices (like disk arrays and tape libraries) to servers.
- Its main job: provide **block-level storage** that looks to the server like a directly attached disk.

Storage Type	Where Storage Is	Access Method	Example Use
<b>DAS</b> (Direct Attached Storage)	Directly connected to a single server	Local connection (SATA, SAS)	Internal hard drives
<b>NAS</b> (Network Attached Storage)	On the network	File-level (via NFS, SMB)	File sharing
<b>SAN</b> (Storage Area Network)	On a separate, dedicated network	Block-level (via Fibre Channel, iSCSI)	Databases, high-performance apps

- A bank with many application servers uses a **SAN** to store customer transaction records.
- All servers can access the same storage pool.
- If one server fails, another can quickly take over without data loss.

# API enabler for cloud computing



- **APIs (Application Programming Interfaces)** act as an **enabler for cloud computing**, allowing users and applications to interact with cloud services securely and efficiently.

## 1. Users & API Clients

- **User:** A person accessing cloud services through a **web browser or application**.
- **API Clients:** Software systems (like apps, scripts, or integrations) that connect to cloud services programmatically.
- Communication happens via **HTTP(S)** and is often secured using **SSL** (Secure Sockets Layer).

## 2. API Communication

- APIs use standard web protocols:
  - **XML-RPC, REST, WebDAV** for structured communication.
  - Common HTTP methods like:
    - **GET** – Retrieve data
    - **POST** – Create data
    - **PUT** – Update data
    - **DELETE** – Remove data

---

### 3. User Apps and Internet-Accessible APIs

- **User Apps and Services:** Front-end interfaces that customers interact with.
- **Internet-Accessible APIs and UIs:** Allow developers and third-party systems to access and control cloud services without using a GUI.

### 4. Cloud Services Layer

The APIs connect to different cloud-based services such as:

- **Database Service** – Manage and query stored data.
- **Queuing Service** – Handle message queues for distributed applications.
- **Identity Service** – Authentication and authorization.
- **MapReduce Service** – Large-scale data processing.
- **Compute Service** – Virtual machines and processing power.
- **Storage Service** – File and block storage.
- **Management Console** – Admin control panel.
- **Accounting, Billing, and Metering** – Usage tracking and cost calculation.

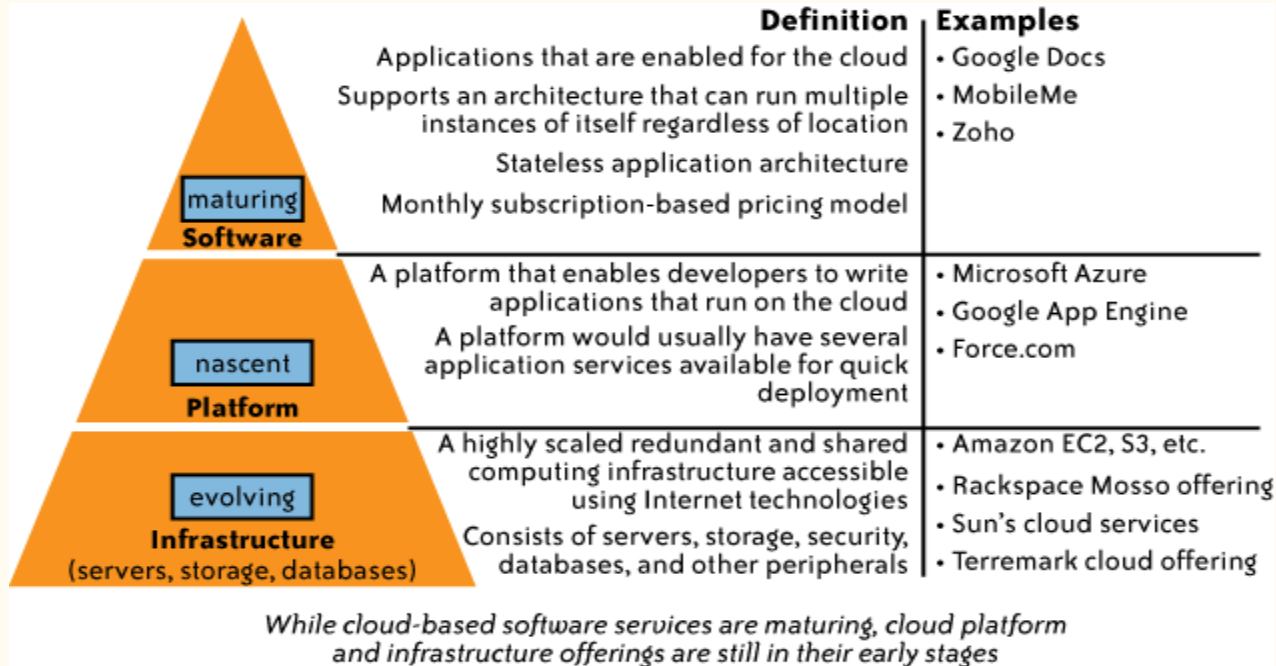
- APIs are the **bridge** between the **user or application** and the **underlying cloud infrastructure**
- They make cloud computing **flexible, programmable, and automatable**, enabling integration with other systems and applications.

- A suitable application programming interface (API) is another enabler for the cloud computing services delivery model
- APIs empower users by enabling features such as **self provisioning and programmatic control of cloud services and resources.**
- Depending on the type of cloud services delivery model (SPI), an API can manifest in different forms, ranging from simple URL manipulations to advanced SOA-like programming models.
- APIs also help to exploit the full potential of cloud computing and mask the complexity involved in extending existing IT management processes and practices to cloud services.

Service-oriented architecture (SOA) is an architectural style that focuses on discrete services instead of a monolithic design.

APIs offered by IaaS cloud service providers (CSPs) **such as Amazon EC2, Sun Cloud, and GoGrid** allow users to create and manage cloud resources, including compute, storage, and networking components.

# The Cloud Services Delivery Model



# The Software-As-a-Service Model



- Traditional methods of purchasing software involved the customer loading the software on his own hardware in return for a license fee (a capital expense, known as CapEx).
- The customer could also purchase **a maintenance agreement** to receive patches to the software or other support services.
- The customer was concerned with the compatibility of operational systems, patch installations, and compliance with license agreements.

- In a **SaaS model**, the customer does not purchase software, but rather rents it for use on a subscription or pay-per-use model (an operational expense, known as OpEx).
- In some cases, the service is free for limited use.
- Typically, the purchased service is complete from a hardware, software, and support perspective.
- The user accesses the service through any authorized device.

# Key benefits of a SaaS model include the following:

1. SaaS enables the organization to outsource the hosting and management of applications to a third party (software vendor and service provider) as a means of reducing the cost of application software licensing, servers, and other infrastructure and personnel required to host the application internally.

## 2.

- **SaaS enables software vendors to control and limit use**, prohibits copying and distribution, and facilitates the control of all derivative versions of their software.
- **SaaS centralized control often allows the vendor or supplier to establish an ongoing revenue stream with multiple businesses and users without preloading software in each device in an organization.**

### 3.

- Applications delivery using the SaaS model typically uses the **one-to-many delivery approach**, with the Web as the infrastructure.
- **An end user can access a SaaS application via a web browser**; some SaaS vendors provide their own interface that is designed to support features that are unique to their applications.

4. A typical SaaS deployment does not require any hardware and can run over the existing Internet access infrastructure. Sometimes changes to firewall rules and settings may be required to allow the SaaS application to run smoothly.

5. Management of a SaaS application is supported by the vendor from the end user perspective, whereby a SaaS application can be configured using an API, but SaaS applications cannot be completely customized.

# The Platform-As-a-Service Model

- In a platform-as-a-service (PaaS) model, the vendor offers a development environment to application developers, who develop applications and offer those services through the provider's platform.
- The provider typically develops toolkits and standards for development, and channels for distribution and payment.
- The provider typically receives a payment for providing the platform and the sales and distribution services.

- PaaS solutions are development platforms for which the development tool itself is hosted in the cloud and accessed through a browser.
- With PaaS, developers can often build web applications without installing any tools on their computer, and can then deploy those applications without any specialized system administration skills.

At a minimum, a PaaS solution should include the following elements:

- A PaaS development studio solution should be browser-based.
- An end-to-end PaaS solution should provide a high-productivity integrated development environment (IDE) running on the actual target delivery platform so that debugging and test scenarios run in the same environment as production deployment
- A PaaS solution should provide integration with external web services and databases.
- A PaaS solution must provide comprehensive monitoring of application and user activity, to help developers understand their applications and effect improvements.

- **Scalability, reliability, and security** should be built into a PaaS solution without requiring additional development, configuration, or other costs
- **A PaaS solution must support both formal and on-demand collaboration** throughout the entire software life cycle (development, testing, documentation, and operations), while maintaining the security of source code and associated intellectual property.
- **A PaaS solution should support pay-as-you-go metered billing.**

*TABLE 2-1. PaaS components*

Client capabilities	Browser-based development tools: Google Web Toolkit, Google Gears, Mashup Editor, Google Gadgets, etc.
Cloud computing services	Cloud-based runtime: EC2, Google App Engine, etc.
General purpose support services	Web services tools: Simple Storage Service, Simple DB, MTurk, GAE Datastore, GDate, Google Accounts, Social Graph API, etc.

## **PaaS platforms also have functional differences from traditional development platforms including:**

- **Multitenant development tools** :Traditional development tools are intended for a single user; a cloud-based studio must support multiple users, each with multiple active projects.
- **Multitenant deployment architecture** Scalability is often not a concern of the initial development effort and is left instead for the system administrators to handle when the project deploys.
  - **In PaaS, scalability of the application and data tiers must be built-in** (e.g., load balancing and failover should be basic elements of the developing platform).

## **Integrated management**

Traditional development solutions (usually) are not associated with runtime monitoring,

but in PaaS the monitoring ability should be built into the development platform.

## **Integrated billing**

PaaS offerings require mechanisms for billing based on usage that are unique to the SaaS world.

Table 2-2 compares the flexibility offered by in-house development platforms and PaaS.

TABLE 2-2. Comparison of in-house and PaaS development platforms

Supported area	In-house development platform	PaaS
Endpoints: desktops, browsers, mobile devices	Most endpoints and clients are supported	Mostly browser-based
Business logic	Multiple vendors are supported	Restricted by PaaS model
Application development framework	Java Platform, Enterprise Edition (Java EE), .NET, etc.	Restricted by PaaS model
Application servers	Multiple vendors are supported	Provided by PaaS
Databases	Multiple vendors are supported	Provided by PaaS
Servers and VMs	Multiple vendors are supported	Provided by PaaS
Storage	Multiple vendors are supported	Provided by PaaS

# The Infrastructure-As-a-Service Model

- In the traditional hosted application model, the vendor provides the entire infrastructure for a customer to run his applications.
- Often, this entails housing dedicated hardware that is purchased or leased for that specific application.
- The IaaS model also provides the infrastructure to run the applications, but the cloud computing approach makes it possible to offer a pay-per use model and to scale the service depending on demand.

## **Features available for a typical IaaS system include:**

### **Scalability**

The ability to scale infrastructure requirements, such as computing resources, memory, and storage (in near-real-time speeds) based on usage requirements

### **Pay as you go**

The ability to purchase the exact amount of infrastructure required at any specific time

### **Best-of-breed technology and resources**

Access to best-of-breed technology solutions and superior IT talent for a fraction of the cost

# IaaS vs PaaS vs SaaS Comparison

ON-PREM	IAAS	PAAS	SAAS
<b>Target Users</b> IT administrators + IT staff	<b>Target Users</b> IT administrators	<b>Target Users</b> Software developers	<b>Target Users</b> End-users
<b>What do you get?</b> Nothing, everything has to be done on-premise	<b>What do you get?</b> Virtual IT data center infrastructure where you install/ manage the OS, software, data + services.	<b>What do you get?</b> Virtual development platform and tools for creating, testing, and deploying your applications.	<b>What do you get?</b> Turnkey software and applications for different business tasks.
<b>Provider controls:</b> Nothing	<b>Provider controls:</b> Servers Storage Virtualization Networking	<b>Provider controls:</b> Servers      OS Storage      Middleware Virtualization Networking      Runtime	<b>Provider controls:</b> Servers      OS Storage      Middleware Virtualization Networking      Runtime Applications Data
<b>User controls:</b> Servers      OS Storage      Middleware Virtualization      Runtime Networking      Applications Data	<b>User controls:</b> OS Middleware Runtime Applications Data	<b>User controls:</b> Data Applications	<b>User controls:</b> Nothing

# Cloud Deployment Models

## Public Clouds

Public clouds (or external clouds) describe cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services, from an off-site, third-party provider who shares resources and bills on a fine-grained, utility-computing basis.

A public cloud is hosted, operated, and managed by a third-party vendor from one or more data centers.

The service is offered to multiple customers (the cloud is offered to multiple tenants) over a common infrastructure



- In a public cloud, security management and day-to-day operations are relegated to the third party vendor, who is responsible for the public cloud service offering.
- Hence, the customer of in the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud.

## Case Study: Dropbox – File Storage & Collaboration in the Public Cloud

- **Background**
- Dropbox is a popular file hosting and collaboration platform with over 700 million registered users. Initially, Dropbox used a mix of **public cloud services** and on-premises infrastructure. Over time, it relied heavily on **Amazon Web Services (AWS)** to scale its file storage and sharing capabilities before eventually building its own hybrid setup.

# Why Public Cloud?

- **Rapid growth:** Needed instant scalability during user expansion.
- **Global accessibility:** Users in different countries require fast file uploads/downloads.
- **Focus on core service:** Avoid building and maintaining physical data centers in early stages.

## Public Cloud Services Used

- **Amazon S3** – Massive, durable storage for user files.
- **Amazon EC2** – Compute power for file indexing, search, and processing.
- **Amazon CloudFront** – Content Delivery Network (CDN) to serve files quickly worldwide.
- **AWS IAM & KMS** – Manage security, authentication, and encryption keys.

## Advantages of Using Public Cloud

- **Scalability** – Easily handles billions of file transactions daily without downtime.
- **Lower upfront cost** – No need to invest in expensive hardware early on.
- **Global reach** – Data replicated across regions for faster access.
- **Security features** – Built-in encryption, identity management, and compliance tools.
- **Faster time-to-market** – Ability to launch services quickly without waiting for infrastructure setup.

## Disadvantages of Using Public Cloud

- **High long-term costs** – Pay-as-you-go can become expensive at scale.
- **Vendor lock-in** – Heavy reliance on AWS meant less flexibility to switch.
- **Data privacy concerns** – Regulatory compliance challenges in certain countries.
- **Network dependency** – Performance tied to internet connectivity and AWS uptime.

## Outcome

- Dropbox used AWS to quickly grow to millions of users.
- Once stable and profitable, Dropbox **migrated most storage to its own infrastructure** ("Magic Pocket") to reduce long-term costs.
- Still uses the public cloud for certain workloads and global distribution.

# Private Cloud

- A **private cloud** is a cloud computing environment dedicated to a single organization.

It can be hosted **on-premises** (inside the company's own data center) or **by a third-party provider** but is not shared with other customers.

## Features:

- Exclusive access and control.
- Customizable for specific workloads.
- Higher security and compliance.
- Usually more costly to build and maintain compared to public cloud.

## Private Clouds

- Private clouds and internal clouds are terms used to describe offerings that emulate cloud computing on private networks.
- These (typically virtualization automation) products claim to deliver some benefits of cloud computing without the pitfalls, capitalizing on data security, corporate governance, and reliability concerns.
- Organizations must buy, build, and manage them and, as such, do not benefit from lower upfront capital costs and less hands-on management.
- The organizational customer for a private cloud is responsible for the operation of his private cloud.

- Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations (i.e., the cloud is dedicated to a single organizational tenant).
- **Variety of private cloud patterns have emerged:**

#### *Dedicated*

Private clouds hosted within a customer-owned data center or at a collocation facility, and operated by internal IT departments

#### *Community*

Private clouds located at the premises of a third party; owned, managed, and operated by a vendor who is bound by custom SLAs and contractual clauses with security and compliance requirements

#### *Managed*

Private cloud infrastructure owned by a customer and managed by a vendor

## **Case Study: NASA Nebula – Private Cloud for Space Research**

NASA developed Nebula, its own private cloud computing platform, to handle the massive data processing needs of space missions and research projects.

### **Why Private Cloud?**

- **Security:** NASA deals with sensitive mission and research data.
- **Customization:** Needed high-performance computing for space simulations and satellite imagery processing.
- **Data Control:** Keep data on U.S. government-controlled infrastructure for compliance.

## Implementation

- Hosted in **NASA's own data centers** at **Ames Research Center**.
- Used **OpenStack** as the cloud management platform.
- Provided Infrastructure-as-a-Service (IaaS) for researchers within NASA and selected partners.

## Advantages

- **High Security & Privacy** -> No external vendor access to sensitive mission data.
- **Custom-Built Performance** → Tuned for computational-heavy workloads like image analysis from Hubble and Mars missions.
- **Regulatory Compliance** → Fully aligned with U.S. government data protection rules.
- **Cost Control at Scale** -> Reduced dependency on commercial cloud vendors.

# Hybrid Cloud

- A **hybrid cloud** combines **public cloud** and **private cloud** resources, enabling data and applications to move between them.  
This model allows organizations to balance **scalability** and **cost-efficiency** of public cloud with the **security** and **control** of private cloud.
- **Features**
- **Flexibility** – Choose where workloads run based on performance, security, or cost needs.
- **Scalability** – Burst into public cloud when private resources are full.
- **Optimized Costs** – Keep sensitive workloads on private cloud, run general workloads on public cloud.

# Case Study: Netflix – Hybrid Cloud for Streaming & Operations

- **Background**
- Netflix uses **AWS (public cloud)** for its streaming platform and **its own private data centers** for content encoding, editing, and internal workloads.

## Why Hybrid Cloud?

- **Global Scalability** – AWS allows Netflix to serve millions of viewers worldwide without owning all infrastructure.
- **Content Security** – Sensitive, unreleased video content is processed in Netflix's private cloud to prevent leaks.
- **Disaster Recovery** – Public cloud ensures service continuity if private systems fail.

## Implementation

- **Private Cloud** – Used in-house for video production, editing, and encoding.
- **Public Cloud (AWS)** – Hosts the user-facing streaming service, recommendation algorithms, and analytics.
- **Data Flow** – Once content is ready, it's uploaded securely to AWS for global distribution.

## Advantages

- **Best of Both Worlds** – Public cloud scalability + private cloud security.
- **Cost-Effective** – Use expensive private infrastructure only where necessary.
- **Improved Reliability** – Failover between environments.

## **Disadvantages**

- **Complex Management** – Requires integration between two infrastructures.
- **Security Challenges** – Data movement between environments must be secured.
- **Skill Requirements** – Staff must manage multiple cloud systems.

Figure 2-10 lists some examples of CSPs.

	<b>Cloud providers</b>	<b>What they offer</b>	<b>Target cloud product segment</b>	
<b>Established organizations</b>	<b>Amazon AWS</b>	Cloud-based infrastructure hosting including storage, Virtual Private Clouds (VPC)	Infrastructure-as-a-service	<i>Service-centric</i>
	<b>Salesforce AppExchange</b>	Cloud-based application hosting	Platform-as-a-service	
	<b>IBM</b>	Cloud infrastructure hosting and related value-added services	Cloud infrastructure	<i>Products and services</i>
	<b>Microsoft</b>	Cloud-based software platform	Application development platform	
	<b>Sun</b>	Cloud infrastructure hosting and related value-added services	Cloud infrastructure	
<b>New entrants</b>	<b>Engine Yard</b>	Platform to run Ruby on Rails applications	Platform-as-a-service	<i>Niche services</i>
	<b>FlexiScale</b>	Cloud hosting platform similar to Amazon's EC2 platform – aimed towards start-ups	Infrastructure-as-a-service	<i>Niche management services</i>
	<b>CohesiveFT</b>	Offers a cloud-based VPN security solution	Cloud security management service	
	<b>RightScale</b>	Cloud management platform; capable of managing cloud infrastructure from multiple providers	Cloud infrastructure management service	

FIGURE 2-10. CSP examples and their respective offerings

# Key Drivers to Adopting the Cloud

1. Small Initial Investment and Low Ongoing Costs
2. Economies of Scale
3. Open Standards
4. Sustainability

## Small Initial Investment and Low Ongoing Costs

- **Advantage: Small Initial Investment & Low Ongoing Costs in Public Cloud**
1. **No Capital Expenditure (CapEx)**
    - In public cloud, companies don't need to buy **hardware, software, or networking equipment**.
    - Eliminates expenses for **servers, storage systems, and IT infrastructure setup**.
    - Reduces the need for **large IT teams** to manage infrastructure.
  2. **Usage-Based Billing (Pay-as-You-Go)**
    - Charges are based on **actual consumption** (compute hours, storage space, bandwidth, etc.).
    - No fixed monthly costs for unused capacity.
    - Aligns costs with demand — cheaper in low-usage periods.

### 3. Lower Barrier to Entry

- Startups and small businesses can launch without **huge upfront investments**.
- Makes enterprise-grade computing accessible to smaller organizations.

### 4. Flexible Contract Terms

- Many providers allow **short-term or on-demand contracts**.
- Contracts can be **terminated or scaled down** in times of hardship.
- Helps manage budgets more efficiently.

### Example

A small e-commerce startup uses **AWS EC2 instances** to run its website:

- Instead of buying ₹20 lakh worth of servers, it rents cloud capacity for ₹10,000/month.
- During festive seasons, it scales up usage; in off-season, it reduces usage — paying only for what's consumed.

# Economies of Scale

- Most development **projects have a sizing phase** during which one attempts to **calculate the storage, processing power, and memory requirements during development, testing, and production.**
- It is often difficult to make **accurate estimates; under- or overestimating** these calculations is typical.
- The lead time for acquiring the equipment to support these estimates can sometimes be lengthy, thus adding to the time necessary to complete the project

With the flexibility that cloud computing solutions offer, companies can acquire computing and development services as needed and on demand, which means development projects are less at risk of missing deadlines and dealing with the unknown

## Case Study: Resource Sizing Challenge Solved with Cloud Computing

- A **mid-sized healthcare analytics company** was developing a new patient data analytics platform.

During the **sizing phase**, the IT team struggled to estimate:

- **Storage requirements for patient records.**
- **Processing power for complex analytics.**
- **Memory needs for real-time dashboards.**
- Their estimates varied widely between **development, testing, and production phases.**

## Problem in Traditional On-Premises Setup

- If they **underestimated** resources → the system would crash under heavy workloads.
- If they **overestimated** → the company would waste money on unused servers.
- **Lead time** for purchasing and configuring hardware was **6–8 weeks**, delaying the project timeline.

## Cloud-Based Solution

- They adopted **Microsoft Azure** as a **public cloud platform**:
- **On-demand provisioning** of virtual machines for development and testing.
- **Auto-scaling** to handle spikes during production without manual intervention.
- **Pay-as-you-go billing** so they only paid for extra resources when needed.

## Outcome

- Development started **immediately** without waiting for hardware procurement.
- No wasted investment on oversized infrastructure.
- Production system scaled automatically during high-demand periods (e.g., government health reporting deadlines).
- Project completion time reduced by **2 months** compared to initial estimates.

# Open Standards in Cloud Computing

- Open standards in cloud computing refer to **publicly available specifications** that ensure **interoperability, portability, and flexibility across** cloud platforms. They allow different systems, tools, and providers to work together without vendor lock-in.

## Modular Architecture

- **Definition:** Cloud systems are built in **independent, interchangeable modules**.
- **Benefits:**
  - Enables **rapid growth** by adding or upgrading components without affecting the whole system.
  - Allows **easy adaptation** to changing user and business needs.
  - Supports **scalability**, making it easier to handle increased workloads over time.
- **Example:** Adding extra storage modules in OpenStack without redesigning the entire infrastructure.

## Case Study: CERN and OpenStack

### Background:

CERN, the European Organization for Nuclear Research, generates petabytes of data every year from particle physics experiments (e.g., the Large Hadron Collider). They needed a highly scalable and flexible cloud infrastructure to store, process, and share data with researchers worldwide.

### Challenge:

- Rapidly increasing data storage and processing requirements.
- Need for **interoperability** with international research institutions.
- Avoiding **vendor lock-in**, since proprietary cloud solutions were too costly and restrictive.

### Solution:

- CERN adopted **OpenStack**, an open-source cloud platform built on open standards.
- Modular architecture allowed them to add more storage and computing power without redesigning the system.
- Open-source community contributions helped CERN continuously improve the system.

## 2. Open Source Software

- **Definition:** Software whose source code is available under licenses in the public domain or meeting official **open-source criteria**.
- **Benefits:**
  - **Free usage** — no licensing fees.
  - **Modifiable** — users can change the code to suit specific needs.
  - **Collaborative improvement** — large global communities contribute bug fixes, features, and security updates.
- **Example:** Kubernetes (open-source container orchestration) is widely adopted in cloud deployments.

### 3. Flexibility and Growth

- **Flexibility:** The ability to **alter source code** ensures continuous optimization and integration with other tools.
- **Growth Potential:** Open-source foundations allow cloud providers and users to **innovate faster**, test new features, and expand services.
- **Example:** OpenNebula allows enterprises to **integrate private and public clouds** seamlessly due to its modifiable source.

#### Summery.....

- Open standards — supported by modular **architecture and open-source software** — **are the backbone of cloud computing innovation. They ensure scalability, interoperability, and freedom from vendor lock-in, enabling continuous improvement and long-term growth.**

# Sustainability in Cloud Computing

Sustainability in cloud computing refers to building and operating cloud infrastructure in an energy-efficient, eco-friendly, and resilient way, ensuring minimal impact on the environment while meeting growing digital demands

1. **CSP Investments:**
2. **Traditional IT Struggles:**
3. **Enhanced Resilience:**

# CSP Investments

Definition: Cloud Service Providers (CSPs) continuously invest in robust infrastructure and advanced technologies.

Impact:

- Creation of resilient and stable environments.
- Use of energy-efficient data centers and optimized hardware.
- Continuous upgrades to meet growing demand and evolving security needs.
- **Example: Google Cloud's investment in renewable-powered data centers for sustainable operations.**

# Case Study: Microsoft Azure – Investment in Green Data Centers

## Background:

Microsoft Azure, a major CSP, manages thousands of data centers worldwide to support cloud services for enterprises and governments.

## Challenge:

- High power consumption from large-scale infrastructure.
- Need to maintain **99.99% uptime** while cutting carbon emissions.
- Rising demand for secure and sustainable cloud solutions.

## Solution:

- Invested in **underwater data centers (Project Natick)** to reduce cooling costs.
- Transitioned to **100% renewable energy by 2025** for all operations.
- Integrated **AI and IoT monitoring** for predictive maintenance and resilience.



## 2. Traditional IT Struggles

- Historically, companies faced:
  - **Single points of failure** (a single server crash could halt services).
  - **Limited scalability** due to fixed hardware capacity.
  - **High maintenance costs** and long upgrade cycles.
- These issues reduced reliability and increased environmental waste from outdated hardware.

## 3. Enhanced Resilience with Cloud

- **Clustering:** Multiple servers work together to handle workloads, reducing the impact of failures.
- **State-of-the-Art Solutions:** Use of automated monitoring, predictive scaling, and AI-driven optimization.
- **Redundancy & Failover:** CSPs replicate data and workloads across multiple regions, ensuring minimal downtime during outages.
- **Example:** AWS Availability Zones ensure services stay up even if one data center fails.

# Case Study: Netflix – Achieving Resilience with Cloud

- Earlier, Netflix ran its services on traditional data centers.
- During peak times, a **single point of failure** (like a server crash) caused long outages, impacting millions of users.
- Scaling was hard because hardware upgrades took time, and maintenance costs were very high.

## Challenge:

- Outages in 2008 caused major disruptions.
- Traditional IT could not handle **unpredictable traffic spikes** (e.g., when new shows were released).
- Reliability was low, and customers lost trust due to downtime.

## Cloud Solution:

- Netflix migrated to **Amazon Web Services (AWS)**.
- **Clustering:** Services were split into microservices running across multiple servers, ensuring no single point of failure.
- **State-of-the-Art Solutions:** Netflix built its own monitoring tools (e.g., *Chaos Monkey*) to test and improve resilience.
- **Redundancy & Failover:** AWS Availability Zones replicated data across regions. If one data center failed, another took over seamlessly.

- Netflix achieved 99.99% uptime globally.
- They scaled automatically to serve over 230+ million users worldwide.
- Maintenance costs reduced, and resilience increased.
- Environmental impact was minimized by using shared cloud infrastructure instead of running large physical data centers.

# **The Impact of Cloud Computing on Users**

This section describes the impact of cloud computing on different types of users:

- Individual consumers
- Individual businesses
- Start-ups
- Small and medium-size businesses (SMBs)
- Enterprise businesses

# Individual Consumers: Cloud in Everyday Life

- **Email and storage:** Most individuals use cloud-based email and storage services (e.g., Gmail, Google Drive).
- **Social networking:** Platforms like Facebook, LinkedIn, and Twitter are cloud-based, storing vast amounts of personal data.
- **Media consumption:** Streaming services (e.g., Netflix, Spotify) and online gaming rely heavily on cloud infrastructure.
- **Privacy concerns:** High volumes of personal data stored in the cloud raise concerns about data privacy and security breaches.
- **Cloud-based applications:** Consumers use cloud apps for fitness tracking, personal finance, and even tax preparation.

## Individual Businesses

- Cloud computing allows individuals to start businesses with **low entry costs** and without investing in expensive hardware.
- Basic **cloud-based tools** (website hosting, storage, email, collaboration tools) are often free or low cost.
- The **expectation** is that essential software should be **nearly free of charge**, with payment only for premium features or extra usage.
- Individuals can:
  - Host websites to attract and serve customers.
  - Sell products on platforms like **eBay or Craigslist**.
  - Use **virtual marketing and online ads** to promote their business.
  - Manage funds through **online banking** and cloud-based accountancy services.
  - Use **virtual assistants** to book appointments, plan schedules, and arrange trips.

- A freelance graphic designer wanted to start her own business with limited budget.
- She could not afford expensive software, servers, or office space.

### **Cloud Adoption**

- Used Google Drive / Dropbox for storing and sharing design files with clients.
- Subscribed to **Canva Pro and Adobe Creative Cloud** on a monthly basis instead of buying costly lifetime licenses.
- Built a portfolio website using Wix (cloud-based hosting) to attract new clients.

# Start-ups and Cloud Computing

## 1. Scalable & Flexible Setup

- When a new business starts, the owner wants operations to be scalable (grow with demand) and flexible (easy to change).
- Cloud services provide this by offering **pay-as-you-go** resources.

## 2. Low Priority for IT Department

- Start-ups usually focus more on **marketing, R&D, and funding**.
- Building a full in-house IT department is costly and not the first priority.
- Cloud allows them to access IT infrastructure without hiring a big team.

## 3. Past vs. Present Approach

- Earlier, **mature IT infrastructure** was seen as a requirement for a company to be ready for **IPO** (Initial Public Offering).
- Now, with cloud, start-ups can **scale quickly without heavy upfront investment**.

## 4. Scalability with ERP

- In the past, companies had to **implement ERP (Enterprise Resource Planning)** on-premise to show scalability.
- Today, with **cloud-based ERP solutions (e.g., SAP, Oracle NetSuite)**, start-ups can scale faster at lower cost.

# Start-ups

When a business owner starts up a new business, he wants to set up operation in a **scalable**, flexible fashion.

Building an IT department is a low priority compared to marketing the product, investing in research and development, or securing the next round of funding.

In the past, a **mature IT infrastructure was a sign that a start-up company was ready for an initial public offering (IPO).**

A company would demonstrate scalability by implementing a robust enterprise resource planning (ERP) solution and hosting it on the premises

Currently, a more common approach is to outsource the majority of IT and maintain a lean IT shop.

The challenge now becomes getting locked into provider contracts and the levels of service that the CSP will face.

Critical success factors are the ability to scale the infrastructure as volume increases, and rapidly modify the service for new product lines, channels, markets, or business models.

# SMBs and Cloud Computing

## 1. Defining SMBs

- Small and Medium Businesses (SMBs) are not just defined by **revenue** but also by **business complexity**.
  - Example: Number of products, countries they operate in, or supply chain integration.
- Larger SMBs usually have **more complex operations** than smaller ones.

## 2. Growth and Legacy Considerations

- SMBs often expand through **acquisitions or spin-offs** from larger firms.
- The **age of the business** matters:
  - Older SMBs may have **legacy systems** and outdated processes.
  - Newer SMBs may start directly with cloud adoption (no legacy burden).

## 3. IT Department Characteristics

- SMBs usually have **smaller IT teams** compared to enterprises.
- IT staff are **less specialized** (one person may handle multiple roles).
- They struggle to justify **big IT investments** like building data centers.
- This often leads to **outdated infrastructure**.
- Cloud computing solves this problem by providing affordable, scalable IT resources.

#### **4. Data Security and Privacy:**

- SMBs have similar data security and privacy requirements as larger enterprises.

#### **5. Decision-Making Structure:**

- Fewer decision-makers compared to larger enterprises, which can streamline or hinder IT decisions.

#### **6. Cloud Computing Opportunities:**

- SMBs can accelerate cloud adoption due to fewer in-house infrastructure constraints.
- Complex SMBs may lead in cloud computing, relying on a mix of Cloud Service Providers (CSPs) for IT services.

# Enterprise Businesses and Cloud Computing

## 1. Expanded Use of Cloud Services

- Mature enterprises are increasingly using cloud platforms.
- Earlier, cloud was mostly used for **basic external services** outside the company firewall.
- Now, enterprises are moving beyond that — integrating cloud into mainstream operations and strategy.

## 2. Cloud for Personal Productivity

- Employees rely on cloud-based tools for **day-to-day activities** such as:
  - Online research
  - Travel bookings
  - Scheduling
- Enterprises also use cloud applications for **non-sensitive corporate tasks**, such as:
  - Employee surveys
  - Internal polls
  - Knowledge-sharing tools
- This boosts efficiency without major security concerns.

### 3. Cloud in Business-Critical Functions

- The **big shift** is the use of cloud for **core enterprise functions** like:
  - **CRM** (e.g., Salesforce.com)
  - **Document management**
  - **Procurement & purchasing**
  - **Logistics & supply chain**
- Even **sensitive data** is being stored and managed in the cloud, showing growing trust in cloud security.

### 4. Security and Privacy Considerations

- Enterprises weigh **security & privacy risks** against **cost benefits** of cloud adoption.
- Best practice: maintain **redundancy** (duplicate data across both cloud and internal systems) to reduce risk of outages or breaches.

## 5. Risks of Vendor Lock-In

- Using one provider's **proprietary architecture** can create dependency.
- This reduces flexibility, increases switching costs, and limits innovation.
- Enterprises need to adopt **open standards & multi-cloud strategies** to avoid lock-in.

## 6. Time to Market as a Key Driver

- Speed is often the **main reason enterprises choose cloud**.
- When time and cost are critical (e.g., launching new products or entering new markets), cloud offers the **fastest, most scalable solution**.
- In many cases, cloud becomes the **only viable option**.

# Governance in the Cloud

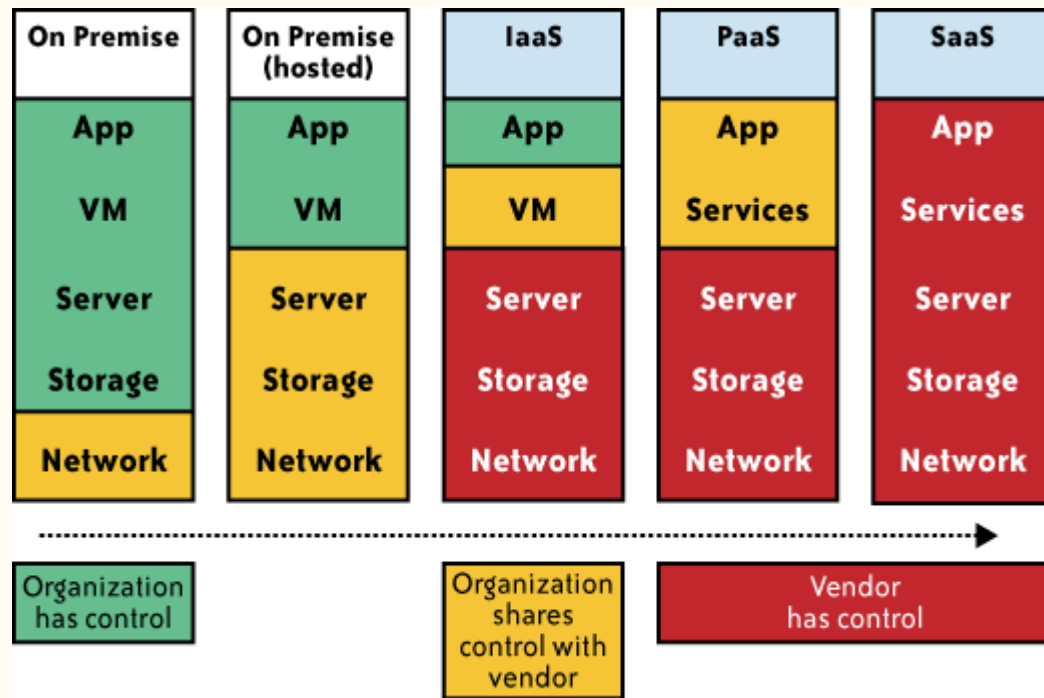
Traditionally, most IT organizations govern the five technology layers shown in the figure.

The two on-premises models indicate that IT has total control over (and responsibility for) all five technology layers.

However, as we move from IaaS to PaaS to SaaS, the IT organization's level of control diminishes and the CSP's level of control increases.

However, although control increases for the CSP, responsibility remains with the IT organization.

It is critical for IT organizations to develop strong monitoring frameworks over the SPI delivery model to ensure that their service levels and contractual obligations are met.



# Barriers to Cloud Computing Adoption in the Enterprise

- **Security Concerns in Cloud Computing**
- **Privacy in Cloud Computing**
- **Connectivity and Open Access**
- **Reliability in Cloud Computing**

**New computing model:** Cloud computing introduces a new paradigm that affects how security is managed.

**Levels of security:**

- **Network Security:** Protecting data as it travels over networks.
- **Host Security:** Safeguarding the physical servers and virtual machines.
- **Application Security:** Ensuring applications are secure from vulnerabilities and attacks.
- **Data Security:** Protecting data at rest and in transit from unauthorized access.

**Uncertainty and Risk:** High levels of uncertainty about how well cloud providers manage these security aspects.

**Executive Concerns:** Security remains the top concern for information executives when considering cloud adoption.

**Security Measures:**

- **Encryption:** Use of encryption to protect data.
- **Access Controls:** Implementing robust access management policies.
- **Regular Audits:** Conducting regular security assessments and audits.

# Security

- **New Computing Model:**

Cloud computing changes how IT resources are delivered and managed. This introduces new **security challenges** across all levels:

- **Network level** → secure data transfer, prevent attacks during communication.
- **Host level** → protect the servers (virtual machines, containers) that run applications.
- **Application level** → ensure cloud apps are free from vulnerabilities like SQL injection, malware, etc.
- **Data level** → protect sensitive data stored and processed in the cloud through encryption, access control, and backups.

- **Uncertainty Factor:**

Since cloud involves **shared infrastructure** and **remote management**, enterprises worry about:

- Who controls the data?
- Can the provider guarantee security?
- How to comply with regulations (GDPR, HIPAA, etc.)?

- **Industry Feedback:**

CIOs and IT executives consistently rank **security as the number one concern** when deciding on cloud adoption—often **above cost savings or performance**.

# Privacy

- The ability of cloud computing to adequately address privacy regulations has been called into question.
- Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

# Connectivity and Open Access

The full potential of cloud computing depends on the availability of high-speed access to all.

Such connectivity, **rather like electricity availability**, globally opens the possibility for industry and a new range of consumer products.

**Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products.**

# Reliability

- Enterprise applications are now so critical that they must be reliable and available to support 24/7 operations.
- In the event of failure or outages, contingency plans must take effect smoothly, and for disastrous or catastrophic failure, recovery plans must begin with minimum disruption.

## **Independence from CSPs**

Examples exist of IT outsourcing contracts that have effectively locked a customer into a service that does not meet current or evolving needs at a speed and cost that are acceptable to meet business goals.

This could be caused by a number of factors, and is a concern if limited options exist for quickly engaging an alternative provider supplier to meet the needs without large transition or penalty costs.

## Changes in the IT Organization

The IT organization will be affected by cloud computing, as has been the case with other technology shifts.

There are two dimensions to shifts in technology. **The first is acquiring the new skill sets to deploy the technology in the context of solving a business problem, and the second is how the technology changes the IT role.**

## Political Issues Due to Global Boundaries

- In the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed.
- Given this variability, different privacy rules and regulations may apply.
- Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional.
- For example, as a result of the USA Patriot Act, Canada has recently asked that its government not use computers in the global network that are operating within U.S. borders, fearing for the confidentiality and privacy of the Canadian data stored on those computers.