

Cloud Services

Cloud Computing

- ▶ Cloud service models SaaS, PaaS and IaaS
- ▶ Basics of Infrastructure Management Services
- ▶ Understand the key benefits of public cloud services
- ▶ Key players of public cloud service providers,
- ▶ Basics of Cloud security models
- ▶ Key challenges in Cloud environments.

Cloud Computing

- ▶ A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications, and services).
- ▶ Cloud model is composed of
 - ▶ Five essential characteristics,
 - ▶ Three service models, and
 - ▶ Four deployment models.

Cloud Computing Service Models

- ▶ three main types of service models
- ▶ Each type of cloud computing provides different levels of
 - ▶ control,
 - ▶ flexibility, and
 - ▶ management so that we select the proper set of services for our needs.

Three Common Cloud Service Models

- ▶ Infrastructure as a Service (IaaS)
- ▶ Platform as a Service (PaaS)
- ▶ Software as a Service (SaaS)

Model



Software as a Service (SaaS)

Especially interesting for private users is cloud-based application software complete with user interface, such as Microsoft Office 365 or Dropbox, Google Drive, OneDrive & Co.



Platform as a Service (PaaS)

Companies can rent predefined platforms for software development, e.g. Microsoft Azure. The provider deals with administration of the underlying servers.



Infrastructure as a Service (IaaS)

Providers like Amazon Web Services (AWS) rent out storage and computing capacities on their servers.

Infrastructure As A Service (IaaS)

- ▶ Most flexible type of cloud service
 - ▶ lets us rent the hardware and
 - ▶ contains the basic building blocks for cloud and IT.
- ▶ gives complete control over the hardware that runs your application
 - ▶ servers,
 - ▶ VMs,
 - ▶ storage,
 - ▶ networks &
 - ▶ operating systems).
- ▶ An instant computing infrastructure, provisioned and managed over the internet.
- ▶ best level of flexibility and management control over our IT resources.
- ▶ like the prevailing IT resources with which many IT departments and developers.

Infrastructure As A Service (IaaS)

- ▶ Examples of IaaS a
 - ▶ virtual Machines or
 - ▶ AWS EC2,
 - ▶ Storage or
 - ▶ Networking.
- ▶ DigitalOcean,
- ▶ Amazon Web Services (AWS),
- ▶ Microsoft Azure,
- ▶ Google Compute Engine (GCE),
- ▶ Rackspace, and
- ▶ Cisco Metacloud.



Benefits of IaaS

- ▶ An efficient and cost-effective way to deploy, operate, and scale your IT infrastructure.
- ▶ Easy to set up and configure
- ▶ Available as a service from an external provider, we don't have to worry about building and maintaining our own infrastructure.
- ▶ Cost savings
 - ▶ We pay only for what we need – storage space, CPU power, bandwidth, and other resources. This makes it easier to scale up or down as needed.
- ▶ On-demand access:
 - ▶ We can instantly provision new resources whenever they're needed without having to invest in new hardware and software or hire additional IT staff members.
 - ▶ The cloud provider takes care of all the maintenance and upgrades required to keep our servers online 24/7 with 99 percent uptime guarantees (or better).
- ▶ Flexibility:
 - ▶ We can easily add more resources when demand increases without having to upgrade equipment or hire more IT professionals.

IaaS Use-Cases

- ▶ useful for backing up, storing, and recovering data, managing fluctuating storage needs.
- ▶ It is cheaper and faster to set up test and development environments.
- ▶ Companies working with Big Data often use IaaS, allows them to increase their computing power.
- ▶ can be an optimal basis for some complex web projects
 - ▶ For sites with fluctuating traffic, as a website hosted in the cloud can profit from the verbosity rendered by a massive network of physical servers and demand scalability to manage unpredictable demands
- ▶ Can be a better alternative for complex tasks which include millions of variables or calculations and, might require the use of supercomputers or clusters.
- ▶ Users can easily access high-end apps with IaaS.
 - ▶ Can run graphic-intensive applications without any latency issues as the cloud servers offer superior performance
 - ▶ have increased productivity because the app will run with great speed.
- ▶ The application deployment over the cloud can be done in less time
 - ▶ Can scale up or down the apps based on unpredictable demands.
 - ▶ All our infrastructure and storage requirements are borne by the providers so that we can easily deploy the applications.

Disadvantages of IaaS

- ▶ Limited infrastructure control
 - ▶ Although IaaS providers normally handle upkeep, upgrades, and management of the underlying infrastructure,
 - ▶ users have less control over the environment and might not be able to make some adjustments.
- ▶ Security issues
 - ▶ Users must take responsibility for protecting their data and apps, which can be very demanding.
- ▶ Restricted access
 - ▶ Owing to legal regulations, cloud computing may not be available in some states or nations.

Platform As A Service (PaaS)

- ▶ a cloud service model that gives a ready-to-use development environment
 - ▶ developers can specialize in writing and executing high-quality code to make customized applications.
- ▶ helps to create an application quickly without managing the underlying infrastructure
 - ▶ when deploying a web application using PaaS, we don't have to install an operating system, web server, or even system updates.
 - ▶ We can scale and add new features to your services.
- ▶ makes the method of developing and deploying applications simpler
- ▶ more expensive than IaaS but less expensive than SaaS.
- ▶ Makes us more efficient as we don't get to worry about resource procurement, capacity planning, software maintenance, patching, or any of the opposite undifferentiated work involved in running your application.

Examples of PaaS

- ▶ Elastic Beanstalk or Lambda from AWS,
- ▶ WebApps,
- ▶ Functions or
- ▶ Azure SQL DB from Azure,
- ▶ Cloud SQL DB from Google Cloud, or
- ▶ Oracle Database Cloud Service from Oracle Cloud.

Benefits of PaaS

- ▶ an easy way to build an application
- ▶ Faster development time
 - ▶ We don't have to build infrastructure before you can start coding.
- ▶ Reduced costs
 - ▶ Our IT department won't need to spend time on manual deployments or server management.
- ▶ Enhanced security
 - ▶ providers lock down our applications so that they're more secure than traditional web apps.
- ▶ High availability
 - ▶ A PaaS provider can make sure our application is always available, even during hardware failures or maintenance windows.

PaaS Use-Cases

- ▶ useful for companies developing, running, and managing app programming interfaces and microservices.
- ▶ Useful for the development of new APIs and complete API management.
- ▶ suitable for setting up and managing an organization's database
 - ▶ offers a scalable, secure, and on-demand platform to create, administer, and maintain databases.
- ▶ PaaS tools
 - ▶ allow for advanced analysis of business data, to identify patterns, make predictions, and ultimately make more qualified and data-driven decisions.
 - ▶ can help companies predict behaviors and events for better planning.
- ▶ supports various programming languages, application environments, and tools, which allows connectivity and integrations required in IoT deployments.
- ▶ can be a delivery mechanism for communication and collaboration which means that features like voice, chat, and videos can be added to applications built on the PaaS cloud service model.

Disadvantages of Paas

- ▶ Limited infrastructure control
 - ▶ Although PaaS providers normally handle upkeep, upgrades, and management of the underlying infrastructure, this might also imply that users have less control over the environment and may not be able to make certain adjustments.
- ▶ Dependency on the provider
 - ▶ Customers rely on the PaaS provider to maintain the platform's scalability, availability, and dependability; however, this poses a risk if the provider encounters disruptions or other problems.
- ▶ Restricted flexibility
 - ▶ The usefulness of PaaS solutions for some organizations may be limited if they cannot handle particular workloads or applications.

Software As A Service (SaaS)

- ▶ SaaS provides us with a complete product that is run and managed by the service provider.
- ▶ software is hosted online and made available to customers on a subscription basis or for purchase in this cloud service model.
- ▶ With a SaaS offering, we don't need to worry about how the service is maintained or how the underlying infrastructure is managed. It would help if you believed how you'd use that specific software.
- ▶ Examples
 - ▶ Microsoft Office 365,
 - ▶ Oracle ERP/HCM Cloud,
 - ▶ Salesforce,
 - ▶ Gmail, or
 - ▶ Dropbox.

Benefits of SaaS

▶ Lower Total Cost of Ownership

- ▶ by eliminating hardware expenses and maintenance costs.
- ▶ no longer a need to buy servers or hire IT professionals to maintain or monitor them,
- ▶ results in fewer upfront costs and reduced maintenance fees over time.

▶ Better Security

- ▶ most services are hosted on secure servers in data centers with 24/7 monitoring,
- ▶ less chance for hackers to gain access or steal our data.
- ▶ makes SaaS a more secure option for storing sensitive information than other options like on-premise software or local servers.

SaaS Use-Cases

- ▶ Pop-up live events are well-suited to SaaS models, specifically live sports and esports tournaments, where the event's temporary nature only requires services for a few hours a day in a week.
- ▶ SaaS brings new benefits for content owners looking to take their content directly to the consumer (D2C), with deployments covering everything from the Customer Management Systems (CMS), subscriber management systems, and user experience.
- ▶ SaaS helps in delivering applications that can be widely distributed and accessed. For example, Google's Gmail is a fully managed email-based application and is most easily accessed over the internet without requiring you to install any software on your local device to be able to use it.

Disadvantages of SaaS

- ▶ Limited customization
 - ▶ SaaS solutions are less customizable than software that is hosted on-premises.
 - ▶ As a result, customers may not be able to customize the program to meet their unique requirements and
 - ▶ Must operate within the platform limitations of the SaaS provider.
- ▶ Dependency on Internet connectivity
 - ▶ Since SaaS solutions are usually cloud-based, a steady Internet connection is necessary for them to operate as intended. Users who need to access the software offline or in places with spotty connectivity may find this troublesome.
- ▶ Security issues
 - ▶ SaaS providers are in charge of ensuring the security of the information kept on their servers, security incidents and data breaches are still a possibility.
- ▶ Limited control over data
 - ▶ Organizations who must maintain stringent control over their data for regulatory or other reasons may be concerned that SaaS providers may have access to a user's data.

Characteristics Of Cloud Service Model

▶ Multi-Tenant

- ▶ an architecture in which a single instance of a software application serves multiple customers. Each customer is called a tenant.

▶ Self-Service

- ▶ a private cloud service where the customer provisions storage and launches applications without an external cloud service provider.
- ▶ users access a web-based portal to request or configure servers and launch applications.

▶ Elastic (Scale-Up | Scale-Down)

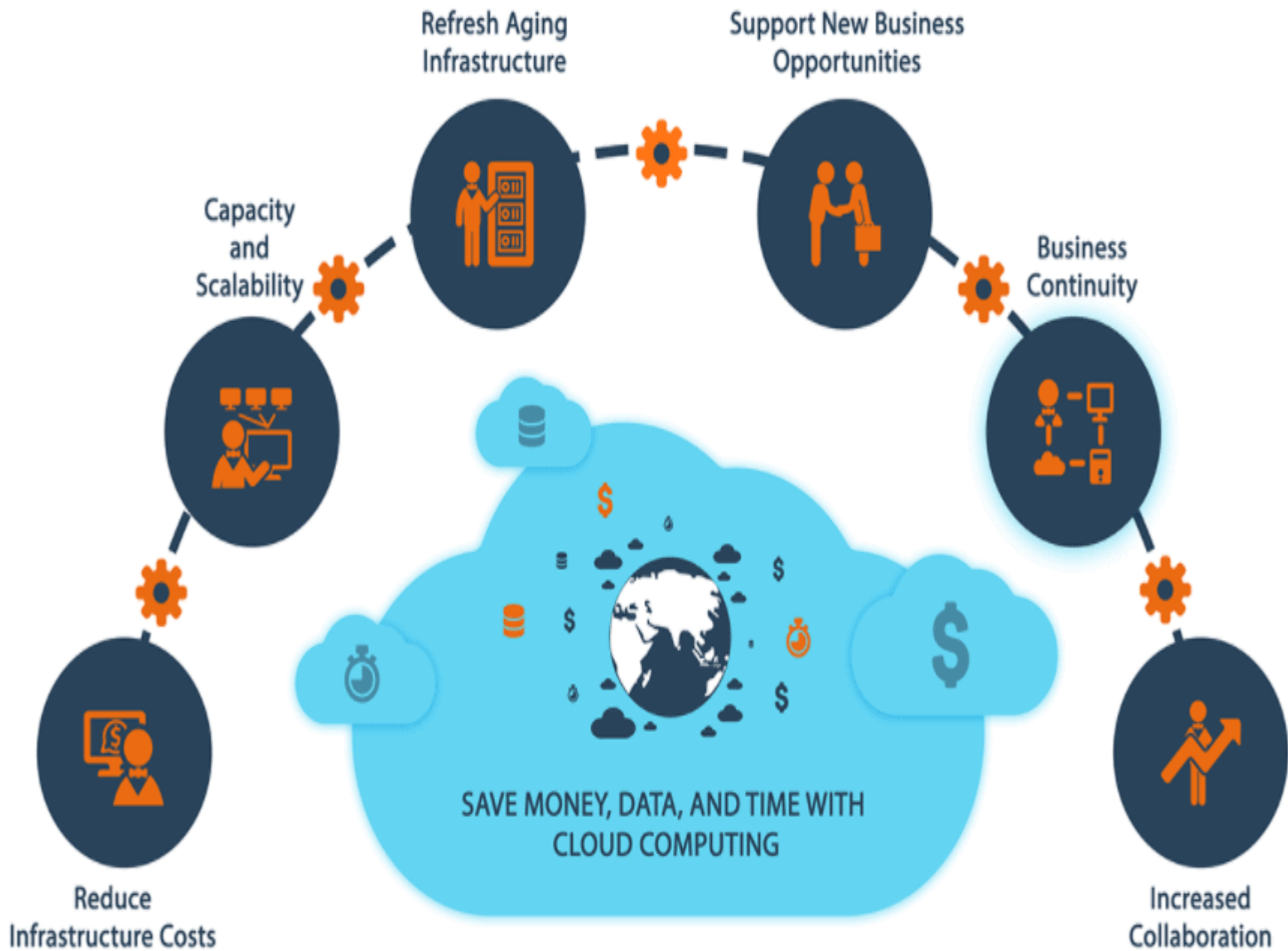
- ▶ the ability to grow or shrink infrastructure resources dynamically as needed to adapt to workload changes in an autonomic manner, maximizing the use of resources.
- ▶ can result in savings in infrastructure costs overall.

▶ Web-Based

- ▶ One can access ones resources via Web-Based applications.

Characteristics Of Cloud Service Model

- ▶ Automated
 - ▶ Most of the things in the Cloud are automated, and human intervention is less.
- ▶ Pay As You Go Model
 - ▶ One has to pay when utilizing cloud resources.
- ▶ Modern Web-Based Integration
 - ▶ allows us to configure multiple application programs to share data in the cloud.
 - ▶ In a network that incorporates cloud integration, diverse applications communicate either directly or through third-party software.
- ▶ Secure
 - ▶ Cloud services create a copy of the data that we want to store to prevent any form of data loss.
 - ▶ If one server loses the data by any chance, the copy version is restored from the other server.





















Cloud Shared Responsibility Model

- Customer Responsibility
- Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Key players to public cloud service providers

 Microsoft Azure	 AWS	 Google Cloud
 Oracle Cloud	 IBM Cloud	 Alibaba Cloud
 Salesforce	 VMware	 DigitalOcean
 Tencent Cloud	 Rackspace	 SAP
 Linode	 OVHcloud	 Adobe Creative Cloud
 Cloud computing	 Huawei	 Dell Technologies

Cloud Security

- ▶ Protect data, applications, and infrastructure stored on the cloud with Cloud security.
- ▶ combination of policies and technologies
 - ▶ that ensure the safety, integrity, and confidentiality of data while it is stored and accessed on the cloud.
- ▶ a critical component of any organization's security strategy
 - ▶ essential for maintaining the security of sensitive data.
- ▶ Solutions and technologies
 - ▶ encryption, authentication, access control, data integrity, data loss prevention, and security monitoring.
- ▶ All of these solutions protect data and applications from unauthorized access, malicious attacks, and data loss.

Cloud Security Models

- ▶ Define types of risks associated with cloud computing and determine the best security measures for protecting data with cloud security models.
- ▶ There are three main cloud security models:
 - ▶ shared responsibility,
 - ▶ multi-tenancy, and
 - ▶ risk-based.

Cloud Security Models

- ▶ The shared responsibility model
 - ▶ most commonly used
 - ▶ the cloud provider is responsible for the security of the cloud infrastructure and
 - ▶ the customer is responsible for the security of their data and applications.
- ▶ The multi-tenancy model
 - ▶ used when multiple tenants use the same cloud infrastructure
 - ▶ where the cloud provider is responsible for the security of the infrastructure and
 - ▶ the tenants are responsible for the security of their own data.
- ▶ The risk-based model
 - ▶ identifies and mitigate the risks associated with cloud computing,
 - ▶ the cloud provider and the customer work together
 - ▶ to identify potential risks and
 - ▶ develop a security strategy to address those risks.

Cloud Security Guidelines

- ▶ a set of best practices that should be followed when using cloud services.
- ▶ These guidelines are designed to ensure the security of data and applications while they are stored and accessed on the cloud.
- ▶ Most important cloud security guidelines include:
 - ▶ Use strong passwords and two-factor authentication
 - ▶ Encrypt data at rest and in transit
 - ▶ Use access control lists to limit access to data and applications
 - ▶ Implement security monitoring and logging
 - ▶ Monitor the security of the cloud infrastructure
 - ▶ Ensure the security of the cloud provider's services
 - ▶ Use secure web protocols
- ▶ Help organizations and individuals can ensure the security of their data and applications while they are stored and accessed on the cloud.

Security Monitoring in Cloud Computing

- ▶ An important part of cloud security.
- ▶ the process of monitoring the security of the cloud infrastructure and the data and applications stored on it.
- ▶ includes activities such as **auditing**, **logging**, and **analyzing** the security of the cloud infrastructure, **monitoring for threats** and **vulnerabilities** and responding to security incidents.
- ▶ essential for ensuring the security of data and applications stored on the cloud.
- ▶ By monitoring the security of the cloud infrastructure, helps organizations and individuals
 - ▶ detect potential threats and take action to prevent them.
 - ▶ identify vulnerabilities and take steps to protect their data and applications.

Benefits of Cloud Security

- ▶ Increased data security
 - ▶ helps protect data from unauthorized access and malicious attacks.
- ▶ can help organizations and individuals
 - ▶ Improved compliance
 - ▶ comply with industry regulations and standards.
 - ▶ Cost savings
 - ▶ by eliminating the need for dedicated hardware and software.
- ▶ Increased productivity
 - ▶ increase their productivity by streamlining processes and reducing manual tasks.
- ▶ Improved scalability
 - ▶ scale their data and applications as needed.

Cloud Security Tips

- ▶ Use strong passwords and two-factor authentication
- ▶ Encrypt data at rest and in transit
- ▶ Implement access control lists to limit access to data and applications
- ▶ Monitor the security of the cloud infrastructure
- ▶ Monitor for threats and vulnerabilities
- ▶ Regularly audit and review security logs
- ▶ Use secure web protocols

Common Challenges

- ▶ Cloud security is not without its challenges.
- ▶ Most common challenges
 - ▶ the lack of visibility into the security of the cloud infrastructure.
 - ▶ Organizations and individuals often do not have the visibility they need to detect potential threats and vulnerabilities.
 - ▶ the complexity of cloud security solutions.
 - ▶ Many of the solutions available are complex and require expert knowledge to implement and maintain.

Best Practices

- ▶ Use strong authentication and authorization
- ▶ Encrypt data at rest and in transit
- ▶ Implement access control lists to limit access to data and applications
- ▶ Monitor the security of the cloud infrastructure
- ▶ Monitor for threats and vulnerabilities
- ▶ Regularly audit and review security logs
- ▶ Use secure web protocols
- ▶ Implement security monitoring and logging
- ▶ Ensure the security of the cloud provider's services

Cloud Security Solutions

- ▶ A variety of cloud security solutions available to organizations and individuals
 - ▶ encryption, authentication, access control, data integrity, data loss prevention, and security monitoring.
 - ▶ designed to protect data and applications from unauthorized access, malicious attacks, and data loss.
- ▶ A variety of cloud security tools and services:
 - ▶ firewalls, intrusion detection systems, web application firewalls, vulnerability scanners, and cloud security assessment tools.
 - ▶ help organizations and individuals identify and mitigate potential threats and vulnerabilities.

Challenges



