Software Defined Systems

Week 12 Cloud Computing and SDS

Lecturer: Biniam Behailu

Addis Ababa Science and Technology University

Addis Ababa, Ethiopia

Contents

Cloud Computing and SDS

Learning objectives

- Understand the fundamental concepts of cloud computing and software-defined systems.
- Identify the benefits and challenges associated with cloud computing.
- Explore the relationship between cloud computing and software-defined technologies.
- Analyze real-world use cases for both cloud computing and software-defined systems.
- Develop strategies for successful implementation and adoption of these technologies.

What is cloud computing?

- Cloud computing refers to the delivery of computing services over the internet, including storage, processing power, and software applications.

- It allows users to access resources and services on-demand, without the need for physical infrastructure or local servers.

Source: http://trivisioninc.com/cloud-services-2/

What is cloud computing?

NIST definition

- *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].*

History of Cloud Computing

1960s
Mainframe computers shared among users.

1990s
Emergence of application service providers (ASPs).

2000s
Introduction to the term "cloud computing

2006s
Launch of Amazon Web Services (AWS).

Key Characteristics cloud computing?

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

On-Demand Self-Service

- Users can provision resources without human intervention.
- **Faster Resource Allocation** - Resources can be deployed instantly, enhancing efficiency.
- **Empowerment for Users** - Users have greater control over their resource management.

Broad Network Access

- Access services over the internet via standard protocols.
- Enables employees to work from anywhere, increasing flexibility.
- Tools and services allow teams to work together seamlessly, regardless of location.
- Users can access services using laptops, tablets, and smartphones, providing versatility and convenience.

Resource Pooling

- Resources are pooled to serve multiple users.
- Maximizes the use of available resources, leading to efficiency.
- Shared resources lower the overall expense for users.

Examples:

- Services like Dropbox and Google Drive allow multiple users to access and store files collectively.
- Cloud platforms like AWS and Azure provide scalable computing resources that can be used by various users simultaneously.

Rapid Elasticity

- Resources can be scaled up or down quickly.
- Resources adjust dynamically to meet user needs.
- Prevents unnecessary costs by aligning resource allocation with actual usage.

Use Cases

- **E-commerce During Sales Events** - Online retailers can quickly increase resources to handle traffic spikes during promotions or sales.

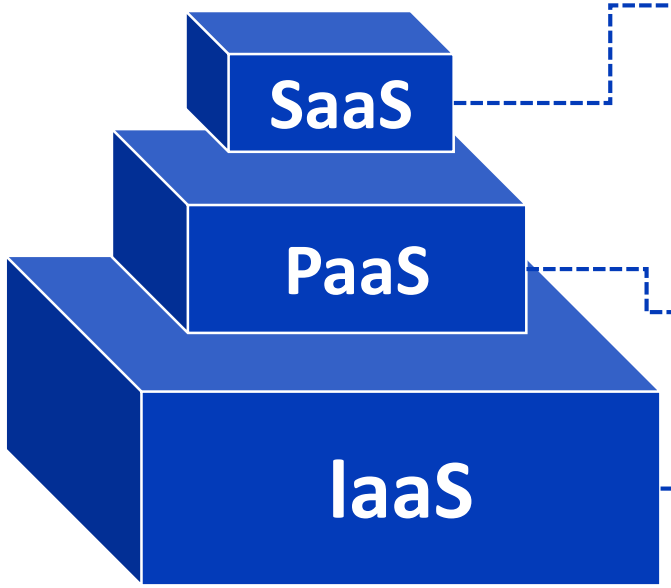
Measured Service

- Usage is monitored and billed based on consumption.
- Users can clearly see how much they are spending based on actual usage.
- Helps users allocate their budgets more effectively by only paying for what they use.

Example

- **Pay-as-You-Go Models** - Services like AWS and Azure charge users based on the resources they consume, allowing for flexible financial planning.

Types of Cloud Services



SaaS - Delivers software applications via the internet, enabling users to access them from any device with a web browser.

PaaS - Offers a platform for developers to create, deploy, and manage applications without worrying about the underlying infrastructure.

IaaS - Provides virtualized computing resources over the internet, allowing users to rent servers, storage, and networks.

Infrastructure as a Service (IaaS)

- Infrastructure as a Service, or IaaS, is a cloud service model that provides virtualized computing resources over the internet.
- Offers scalable storage options for data and applications and networking tools for connectivity and management
- This model offers significant benefits, including cost savings, as businesses only pay for what they use and avoid large capital expenditures on equipment.
- **Examples**: AWS EC2, Microsoft Azure VMs.

Platform as a Service (PaaS)

- Platform as a Service, or PaaS, is a cloud service that provides a platform allowing developers to build, deploy, and manage applications without the complexities of managing the underlying infrastructure.
- Provides integrated tools for coding, testing, and deploying applications.
- Facilitates communication and data management between applications.
- Includes tools for creating and managing databases easily.
- Streamlines development, enhances collaboration.
- **Examples**: Google App Engine, Heroku.

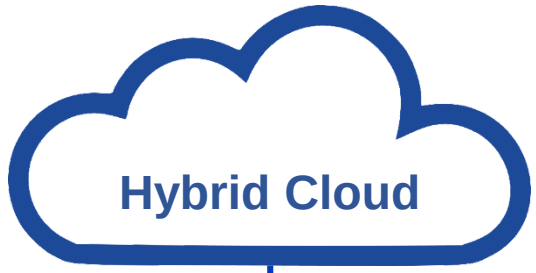
Software as a Service (SaaS)

- Software as a Service, or SaaS, is a cloud service model that delivers software applications over the internet.
- Users can access applications from any device with an internet connection.
- Software is automatically updated, ensuring users have the latest features and security patches.
- The advantages of SaaS are manifold. For users, it offers ease of access from anywhere, automatic updates, and reduced IT overhead, as the provider manages the infrastructure and software.
- **Examples**: Salesforce, Microsoft 365.

Deployment Models

Resources are owned and operated by third-party cloud service providers and delivered over the internet.

Cloud infrastructure dedicated to a single organization, either managed internally or by a third party.



Combines public and private clouds, allowing data and applications to be shared between them.

Cloud infrastructure shared by several organizations with common concerns, such as security or compliance.

Public Cloud

- The public cloud is a cloud deployment model that is owned and operated by third-party providers, making services available to anyone over the internet.
- Reduces capital expenditures by eliminating the need for physical infrastructure.
- Easily adjusts resources to meet varying demand and workloads.
- Ensures services are consistently available with minimal downtime.
- **Examples**: Amazon Web Services (AWS), Google Cloud Platform.

Private Cloud

- A private cloud is a cloud deployment model dedicated to a single organization, providing enhanced security and control over data and applications.
- Offers a higher level of security tailored to the organization's needs.
- Allows for specific configurations to meet unique business requirements.
- Deployment options include local data centers or third-party hosting.
- **Use Cases**: Financial institutions, healthcare organizations.

Hybrid Cloud

- The hybrid cloud is a versatile deployment model that combines both public and private cloud environments, allowing organizations to take advantage of the benefits of both.
- Allows organizations to choose where to run applications and store data.
- Sensitive information can be kept in a private cloud while leveraging public cloud resources for less critical tasks.
- Easily scales up or down depending on workload requirements.
- **Scenarios**: Temporary workloads, data backup.

Community Cloud

- The community cloud is a cloud deployment model that is shared by several organizations with common concerns, such as security, compliance, or performance requirements.
- Facilitates cooperation among organizations working on shared projects or goals.
- Reduces individual costs by distributing expenses across multiple users.
- Tailored to meet the regulatory and compliance requirements of the participating organizations.
- **Examples**: Research institutions, government agencies.

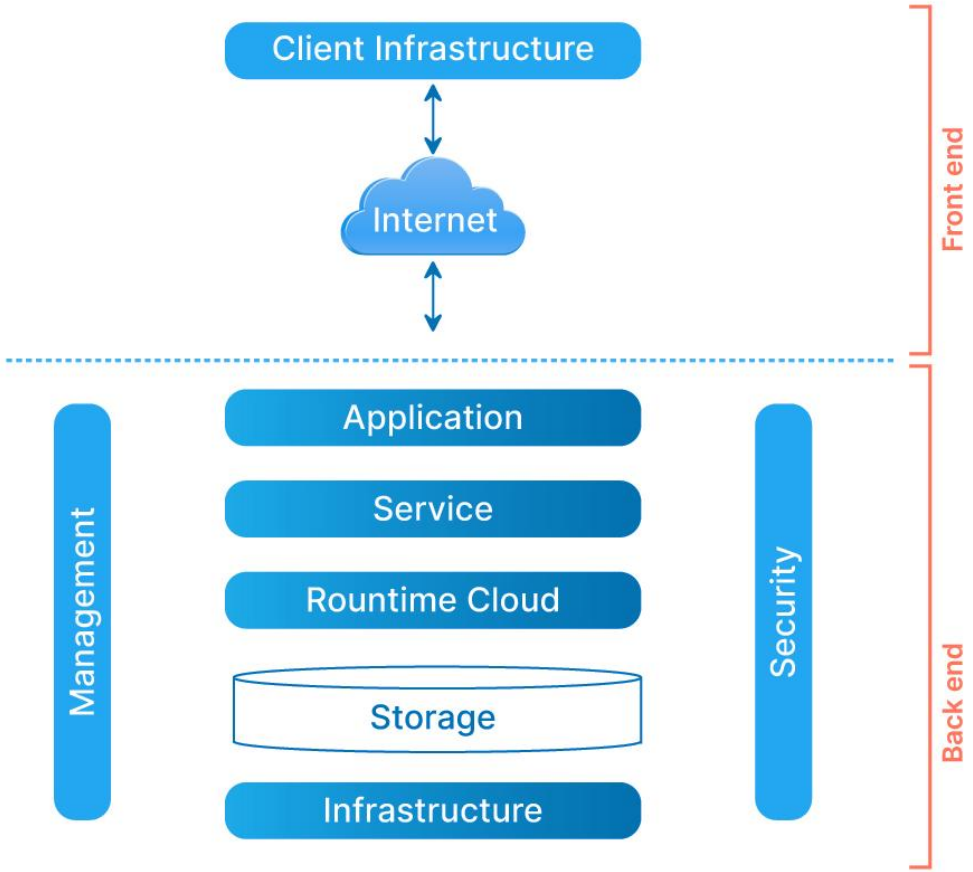
Benefits of Cloud Computing

- **Cost Savings**: Reduces infrastructure costs by using pay-as-you-go models.
- **Scalability**: Easily adjusts resources to meet fluctuating demands.
- **Flexibility**: Offers diverse services and deployment options tailored to specific needs.
- **Performance**: Delivers high-performance computing for efficient application operation.
- **Security**: Implements strong security measures to protect data and ensure compliance.

Common Cloud Computing Use Cases

- **Data Storage and Backup**: Store and back up large amounts of data securely.
- **Software Development and Testing**: Rapidly create and deploy applications in a scalable environment.
- **Web and Mobile Applications**: Host web and mobile applications in the cloud for global accessibility.
- **Big Data Analytics**: Process and analyze vast amounts of data using cloud resources.
- **Disaster Recovery**: Maintain data backups and recovery plans in the cloud for business continuity.

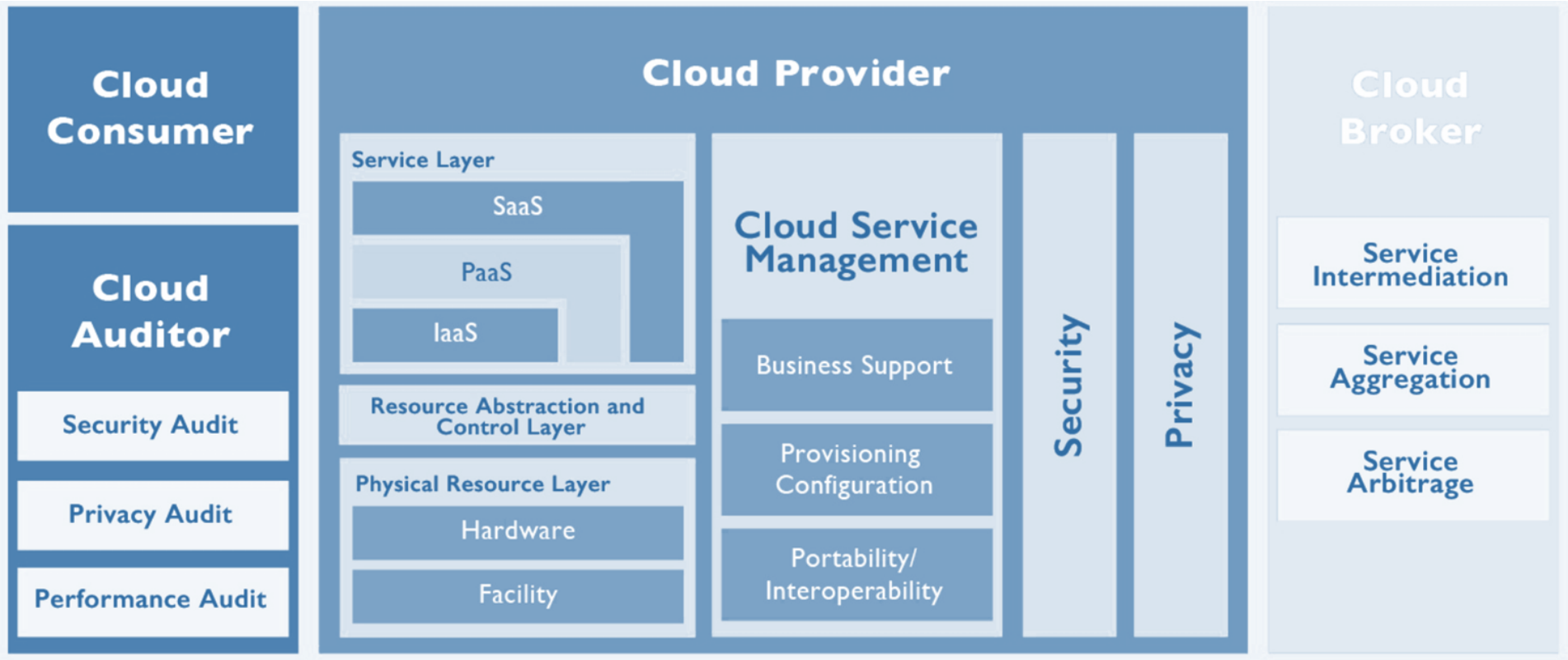
Cloud Architecture



- Cloud architecture refers to the design and structure of cloud computing environments, including the arrangement of components and the relationships between them.
- It involves various elements that work together to deliver cloud services and ensure reliability, scalability, and security.

Source: https://www.shiksha.com/online-courses/articles/cloud-computing-architecture-advantages-and-disadvantages/

NIST Architecture of Cloud



Source: https://cyberrisk-countermeasures.info/2021/12/08/nist-cloud-computing-reference-architecture-and-taxonomy/

Challenges of Cloud Computing

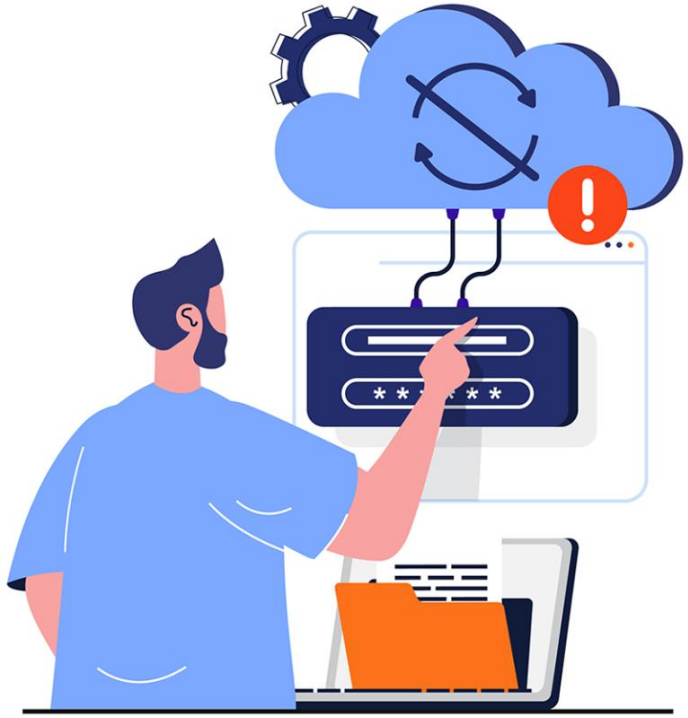
- **Data Security and Privacy Concerns**: Ensuring the protection of sensitive information is critical, as data breaches can have severe consequences.
- **Potential Downtime and Service Outages**: Reliance on cloud services means that any disruption can impact business operations, leading to lost productivity and revenue.
- **Compliance with Regulations**: Organizations must navigate complex regulations regarding data management and privacy, which can vary by industry and location.
- **Vendor Lock-In Risks**: Switching between cloud providers can be challenging and costly, limiting flexibility and negotiation power for organizations.

Data Security

- Safeguarding confidential data is essential for maintaining trust and integrity in business operations.
- Effective data security measures help mitigate the risk of unauthorized access, which can lead to significant financial and reputational damage.

Source: https://www.datasunrise.com/knowledge-center/database-security/

Downtime



- Downtime can result from various factors such as cyberattacks, system failures, hardware malfunctions, and natural disasters.
- Impact on Business Operations: Interruptions can lead to lost productivity, decreased revenue, and damage to customer trust and reputation.

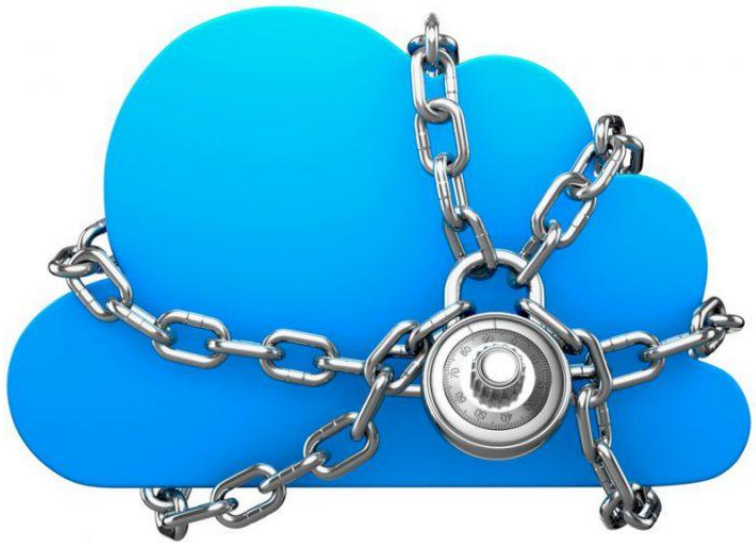
Source: https://hystax.com/navigating-cloud-downtime-steps-to-take-when-services-are-unavailable/

Compliance Issues

- Compliance with regulations such as HIPAA and GDPR is crucial for organizations to avoid legal penalties and maintain operational integrity.
- Ensuring compliance helps safeguard sensitive customer information, fostering trust and loyalty among clients.

Source: https://www.vecteezy.com/vector-art/4579165-flat-isometric-vector-illustration-it-compliance-server-and-cloud

Vendor Lock-In



- Dependency on a specific cloud provider's services and technologies, making it challenging to switch providers or integrate alternative solutions.

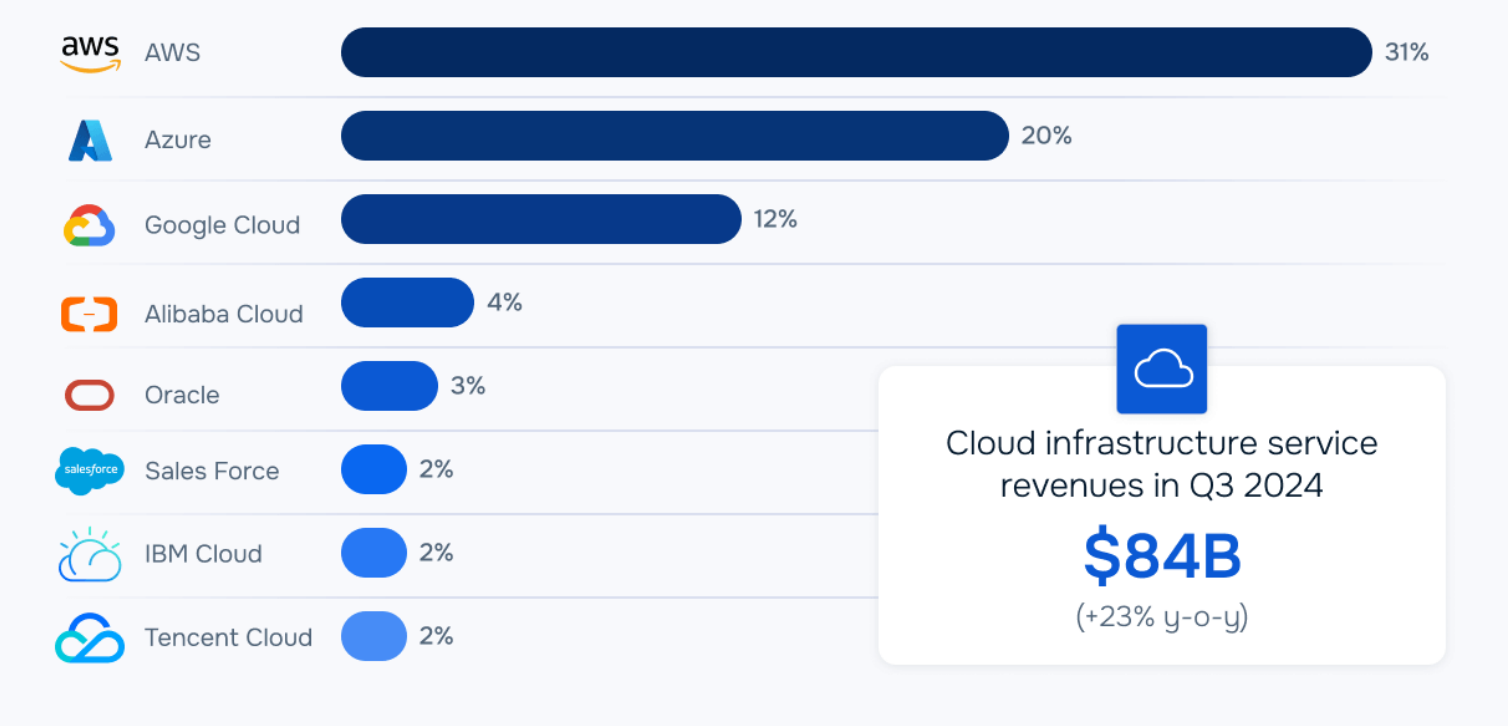
Source: https://infolific.com/technology/moving-to-cloud-avoid-vendor-lock-in/

Industry Applications

- **Healthcare**: Patient data management and telemedicine.
- **Finance**: Risk management and compliance solutions.
- **Education**: E-learning platforms and resource sharing.

Cloud Service Providers

Cloud Market Share Trends



- Worldwide market share of leading cloud infrastructure service providers as of Q3 2024

Source: https://www.emma.ms/blog/cloud-market-share-trends

Economic Models

Cost Categories

- Direct costs (e.g., subscriptions, usage fees)
- Indirect costs (e.g., training, management)

Value Metrics

- ROI
- Total Cost of Ownership (TCO)
- Cost per Transaction

Total Cost of Ownership (TCO)

- Comprehensive assessment of direct and indirect costs.
- Components
  - Infrastructure costs
  - Operational costs
  - Support and maintenance costs

Pay-as-You-Go Model

- Pay-as-you-go (PAYG) is a pricing model where users pay only for the resources and services they actually consume.
- This model is commonly used in cloud computing, utilities, and subscription services.
- This model is especially advantageous for organizations with variable workloads, such as seasonal businesses or startups experiencing rapid growth.

Service Level Agreements (SLAs)

- A Service Level Agreement (SLA) is a formal document that outlines the expected level of service between a cloud service provider and a customer.
- It defines specific metrics, responsibilities, and guarantees regarding service performance.
- Detailed description of the cloud services provided (e.g., infrastructure, platform, software).
- Metrics used to measure service performance, including:
- Availability/Uptime - Percentage of time the service is operational (e.g., 99.9% uptime).
- Response Time - Expected time for the service to respond to requests.
- Throughput: Amount of data processed in a given time frame.

Cloud Security

- Measures and protocols designed to protect data, applications, and infrastructure in cloud environments.

Data Protection

- Encryption of data at rest and in transit.
- Access controls and authentication mechanisms.

Identity and Access Management (IAM)

- User authentication and authorization.
- Role-based access controls (RBAC).

Network Security

- Firewalls, intrusion detection and prevention systems.
- Virtual Private Networks (VPNs) and secure APIs.

Compliance and Governance

- Adherence to regulatory standards (e.g., GDPR, HIPAA).
- Regular audits and assessments.

Shared Responsibility Model

- A framework that delineates the security responsibilities of cloud service providers (CSPs) and their customers.

Responsibilities of Cloud Service Providers

- **Physical Security** - Protection of data centers and infrastructure.
- **Network Security** - Securing the cloud infrastructure against attacks.
- **Platform Security** - Ensuring the security of the cloud services and underlying software.

Shared Responsibility Model

- A framework that delineates the security responsibilities of cloud service providers (CSPs) and their customers.

Responsibilities of Customers

- **Data Security** - Managing data encryption and access controls.
- **Identity and Access Management (IAM)** - Implementing user authentication and permissions.
- **Application Security** - Securing applications deployed in the cloud.

Cloud Computing & Software-Defined Systems

- Cloud services leverage software-defined technologies for scalability and flexibility.
- SDN and SDS improve the management of cloud resources.
- Software-defined systems optimize cloud operations.

Conclusion and Call to Action

- Cloud computing enhances efficiency, scalability, and collaboration.
- Software-defined systems provide flexibility and improved resource management.
- Integration of both technologies drives innovation and operational excellence.
- Continued evolution of cloud services and software-defined technologies.
- Importance of strategic adoption to leverage full potential.

Test Your Knowledge

1. Which of the following cloud service models provides the highest level of control over the underlying infrastructure?

A) Software as a Service (SaaS)

B) Platform as a Service (PaaS)

C) Infrastructure as a Service (IaaS)

D) Function as a Service (FaaS)

Test Your Knowledge

1. Which of the following cloud service models provides the highest level of control over the underlying infrastructure?

A) Software as a Service (SaaS)

B) Platform as a Service (PaaS)

C) Infrastructure as a Service (IaaS)

D) Function as a Service (FaaS)

Reason: IaaS provides the highest level of control because it allows users to manage virtualized computing resources, including servers, storage, and networking, while the cloud provider manages the underlying hardware.

Test Your Knowledge

2. What is a primary characteristic of Public Cloud deployment models?

A) Exclusive access to resources

B) Managed by a single organization

C) Resources are shared among multiple users

D) Requires significant upfront investment

Test Your Knowledge

2. What is a primary characteristic of Public Cloud deployment models?

A) Exclusive access to resources

B) Managed by a single organization

C) Resources are shared among multiple users

D) Requires significant upfront investment

Reason: Public clouds are designed to provide resources and services to multiple customers over the internet, sharing the underlying infrastructure and reducing costs. This model allows users to benefit from economies of scale without needing to invest in physical hardware.

Test Your Knowledge

3. Which one is the key benefits of using a Hybrid Cloud model?

A) Complete isolation of resources

B) Greater control over local data

C) Exclusive use of a single vendor

D) Simplified compliance with regulations

Test Your Knowledge

3. What is one of the key benefits of using a Hybrid Cloud model?

A) Complete isolation of resources

B) Greater control over local data

C) Exclusive use of a single vendor

D) Simplified compliance with regulations

Reason: A hybrid cloud model combines both public and private cloud environments, allowing organizations to maintain greater control over sensitive data and applications while still benefiting from the scalability and cost-effectiveness of public cloud resources.

References

1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, Sep. 2011. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/145/final. [Accessed: May. 27, 2025].

Thank you!

Lecturer: Biniam Behailu

Addis Ababa Science and Technology University

Addis Ababa, Ethiopia