DIHSÜD

FH JOANNEUM University of Applied Sciences
IT & Mobile Security

Cloud Computing

Manfred Pamsl
Institute of Internet Technologies & Applications
IT & Mobile Security

About Me

- **Manfred Pamsl**

- Study of technical mathematics / computer science, TU-Graz
- Software Development and IT solutions for telco industry
- Teaching and research focus
  - Cloud computing
  - Secure server infrastructure

What is Cloud Computing ?

Cloud Computing is the on-demand provisioning of (virtual) computing resources over the network

- Salesforce.com (1999), Amazon Web Services (2003), Amazon Elastic Computing 2 (2006), Google Docs (2006), Microsoft Azure (2010), Apple iCloud (2011), …
- Not a new technology: based on server/network/storage virtualization, broadband network access, multi-client capable software and service-oriented architecture (SOA)

Cloud Computing Definitions

- **NIST SP 800-145**
  - “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.”
- **ISO/IEC 17788:2014**
  - “Cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.”

NIST: Essential Characteristics

- **On-Demand Self-Service**
  - Computing capabilities are unilaterally provisioned by the consumer without requiring human interaction with the service provider
- **Broad Network Access**
  - Capabilities are available over the network and accessed through standard mechanisms
- **Resource pooling**
  - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model
  - The customer generally has no control or knowledge over the exact location of the provided resources

NIST: Essential Characteristics

- **Rapid elasticity**
  - Capabilities can be elastically provisioned and released
  - To the consumer, the capabilities available for provisioning often appear to be unlimited
- **Measured service**
  - Cloud systems automatically control and optimize resource use by leveraging a metering capability
  - Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized services

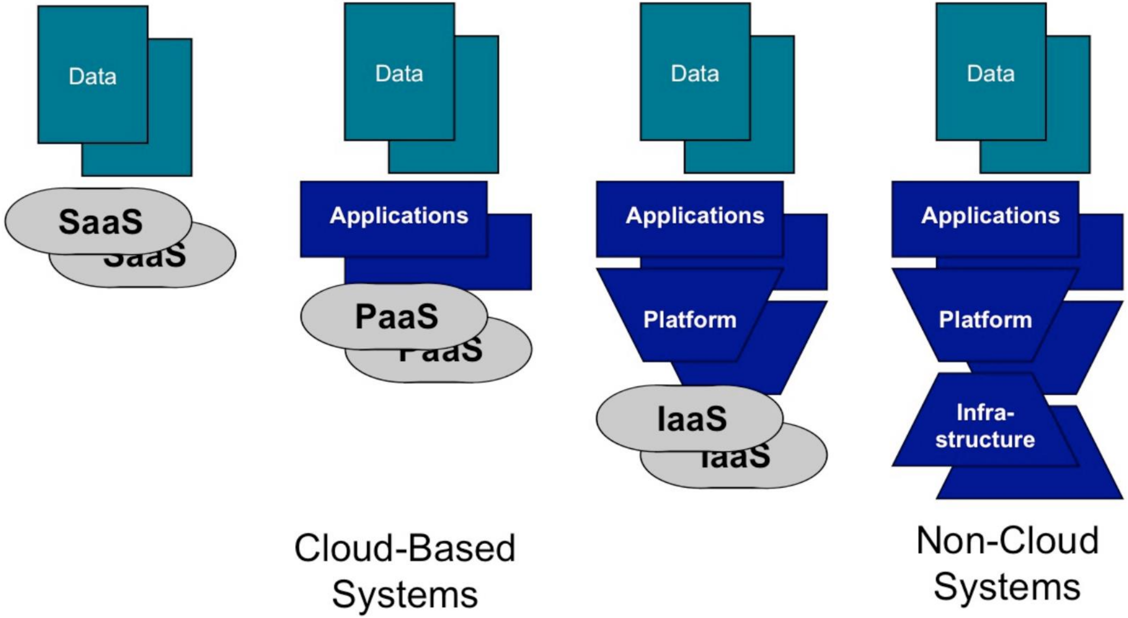
NIST: Service Models

- **Software as a Service (SaaS)**
  - Consumer uses the provider’s applications running on a cloud infrastructure
  - The consumer does not manage or control the underlying cloud infrastructure
- **Platform as a Service (PaaS)**
  - Consumer deploys applications onto the cloud infrastructure using programming languages, libraries, services, and tools supported by the provider
  - Consumer has control over the deployed applications and possibly configuration settings for the application-hosting environment
- **Infrastructure as a Service (IaaS)**
  - Consumer is to provision processing, storage, networks, and other fundamental computing resources
  - Consumer has control over operating systems, storage, and deployed applications and possibly limited control of networking components (e.g. host firewalls)

Additional Service Modells

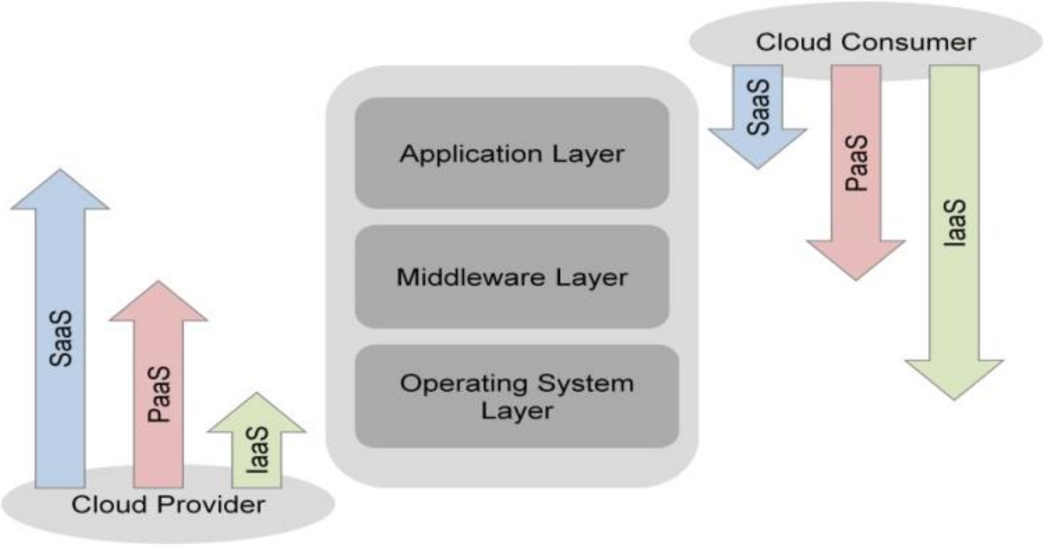
- Additional service model terms may also be used for more specific services, e.g.
  - **Backend as a Service (BaaS)**
    - Provides backend services for (mobile) applications, e.g. notification services, social networks, cloud storage
    - Google Firebase, …
  - **Function as a Service (FaaS, "Serverless Computing")**
    - Event-driven computing execution model
    - Functions (business logic) are executed in stateless containers
    - AWS Lambda, Google Cloud Functions, MS Azure Functions, OpenWhisk, …

Cloud Service Architecture



Source: https://publications.opengroup.org/g135

Cloud Service Control Scope

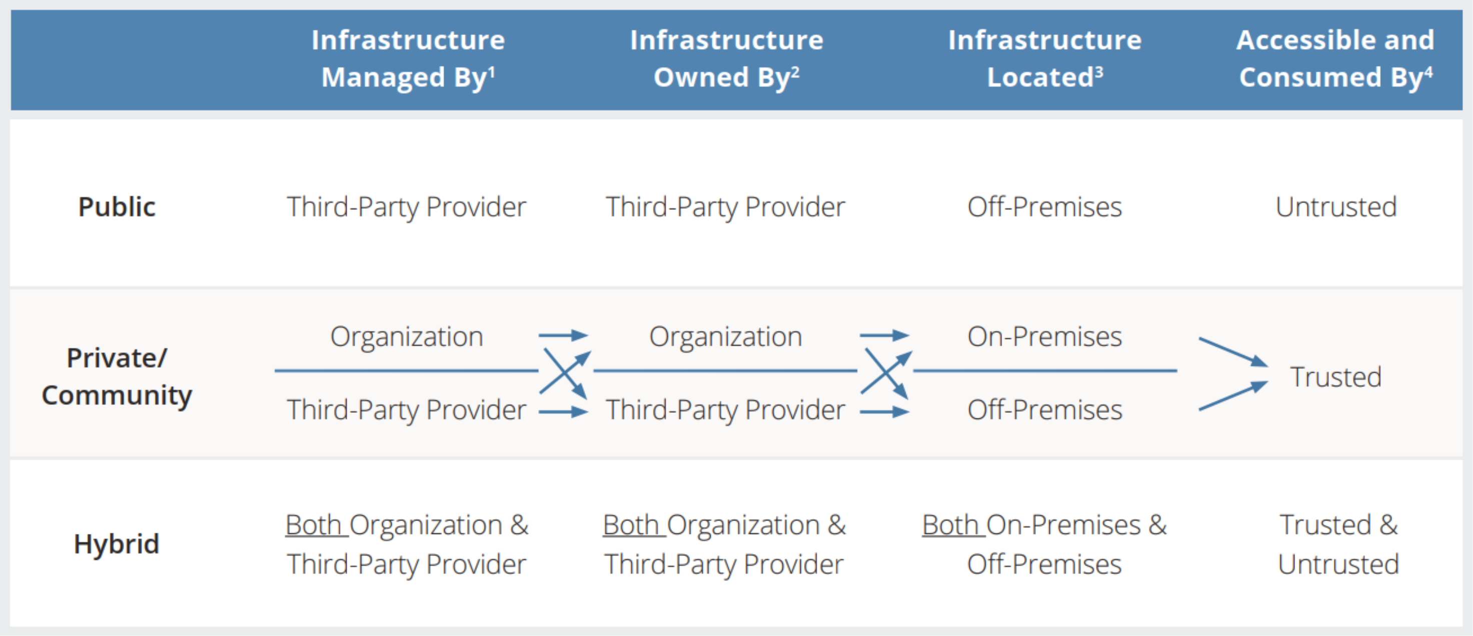


Source : https://www.nist.gov/publications/nist-cloud-computing-reference-architecture

NIST Deployment Models

- **Private Cloud**
  - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units)
  - It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises
- **Community Cloud**
  - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns
  - It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises
- **Public Cloud**
  - The cloud infrastructure is provisioned for open use by the general public
  - It exists on the premises of the cloud provider
- **Hybrid Cloud**
  - The cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound together

Deployment Modells: Management

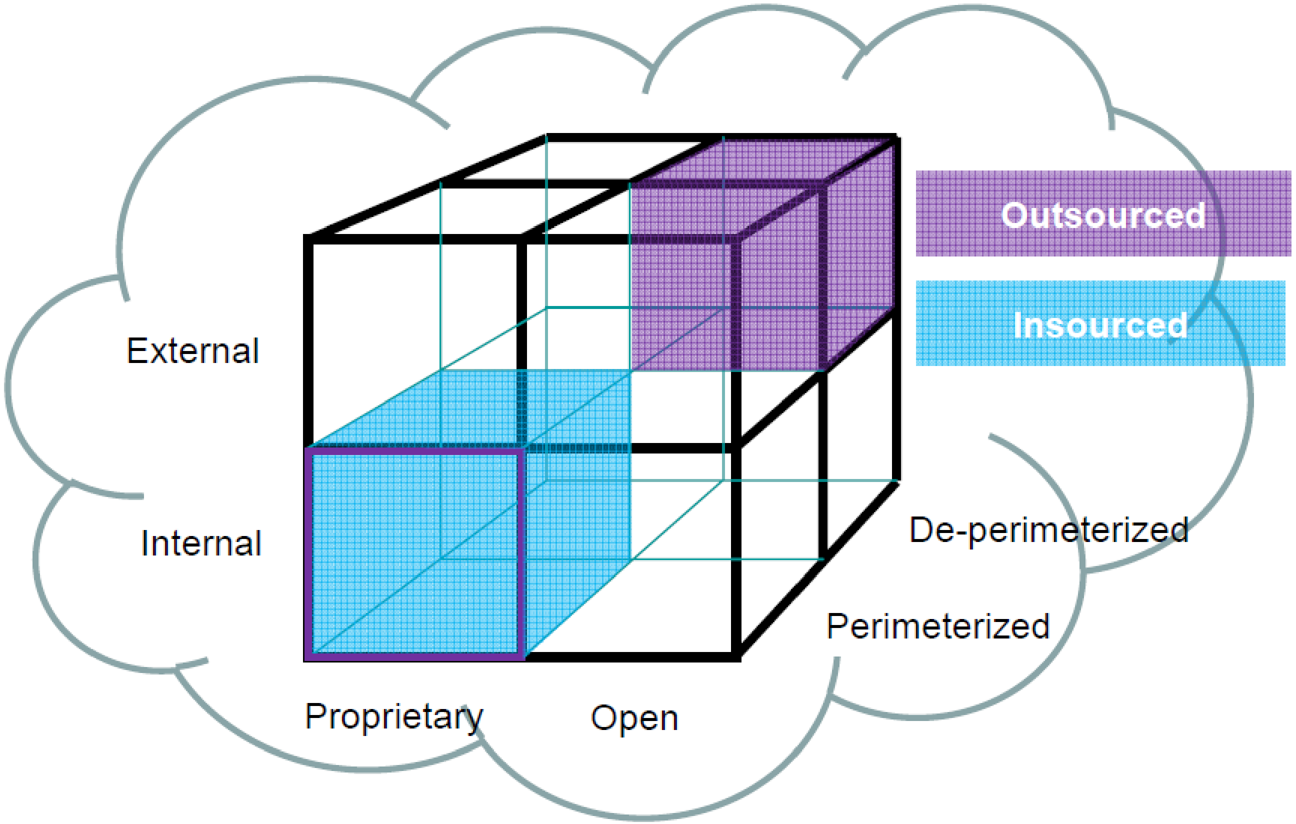


	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization Third-Party Provider	Organization Third-Party Provider	On-Premises Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL-feb27-18.pdf

OpenGroup Jericho Cube Model (1)

- Four criteria (dimensions) to differentiate cloud formations
  - **Physical location of data**: Internal, External
    - Inside or outside of the organization's boundaries
  - **Ownership**: Proprietary, Open
    - Concerning technology, interoperability, data transfer
  - **Security boundary**: Perimeter-iced, De-Perimeter-iced
    - Inside or outside of a security boundary like firewall
  - **Sourcing**: In-sourced, Out-sourced
    - Provided by third party or under control by own staff

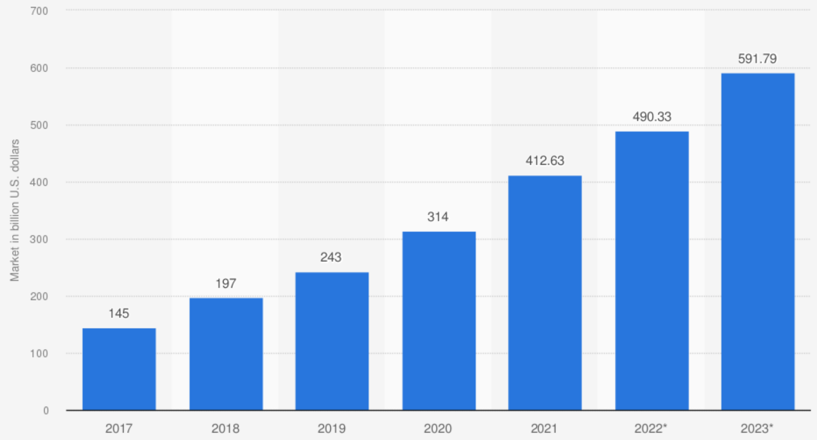


Source : https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Public Cloud Computing Market

https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/

Public cloud services end-user spending worldwide from 2017 to 2023 (in billion U.S. dollars)

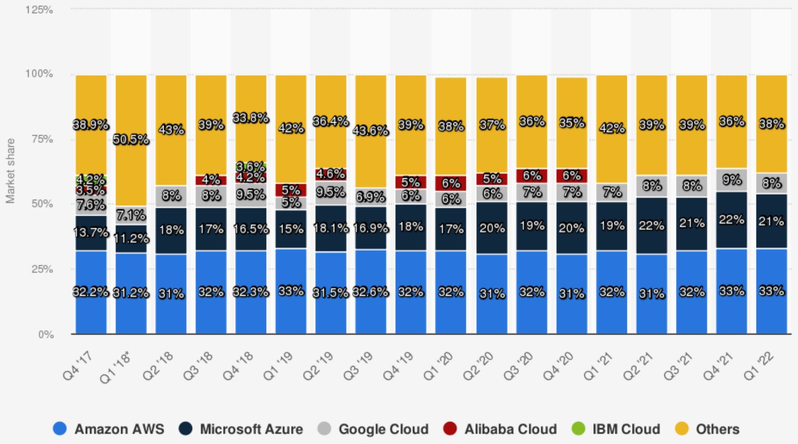


Source
Gartner
© Statista 2022

Additional Information:
Worldwide; 2017 to 2022

https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/

Cloud infrastructure services vendor market share worldwide from 4th quarter 2017 to 1st quarter 2022



Sources
Canalys; Statista
© Statista 2022

Additional Information:
Worldwide; 2017 to 2022

Using a Public Cloud – Potential Advantages

- Lower up-front investments
  - A big portion of the IT budget becomes an operating expense rather than an upfront capital expenditure
- Cost efficiency
  - Public cloud providers are running the services very efficiently
- Highly elastic capacity
  - Easy to expand, but may also be ramped down during periods of light demand
- Simplified maintenance and upgrades
  - Resources and updates can be deployed in an automated, standardized fashion
  - No need to physically maintain servers or data center facilities

Using a Public Cloud – Potential Disadvantages

- Compliance issues
  - Multinational jurisdiction and standards
- Network latency and bandwidth of WAN connections
  - Application response time
- Provider lock-in
  - Restricted portability for data, applications and services
- Security risks
  - Loss of governance, control is ceded to the provider
  - Virtualization isolation failure (e.g. by Meltdown/Spectre vulnerabilities)
  - Insecure or incomplete data deletion by the provider
  - Management interface usually accessible over the Internet
  - …

OWASP Top 10 Cloud Security Issues (1)

- **Accountability and Data Ownership**
  - Risk: Third party stores and transmits data
  - Mitigation: Vendor shall have a set of security policies that map to your own

- **User Identity Federation**
  - Risk: Loose control over user identities when services are moved to different cloud providers by creating mutiple islands of identities
  - Mitigation: Users should be uniquely identifiable with a federated authentication (e.g. Security Assertion Markup Language, SAML) that works across the cloud providers

https://owasp.org/www-pdf-archive/OWASP_Cloud_Top_10.pdf
https://hitachi-systems-security.com/the-top-10-owasp-cloud-security-risks

OWASP Top 10 Cloud Security Issues (2)

- **Legal & Regulatory Compliance**
  - Risk: Complex to prove regulatory compliance, especially across geographical jurisdiction
  - Mitigation: Choose a cloud provider who provides a solution for different data protection laws

- **Business Continuity & Resiliency**
  - Risk: Responsibility of business continuity gets delegated to the cloud provider
  - Mitigation: Make sure that the SLAs cover data resilience and protection

OWASP Top 10 Cloud Security Issues (3)

- **User Privacy & Secondary Usage of Data**
  - Risk: User's personal data gets stored in the cloud as users start using social web sites, most of the social sites are vague about how they will handle users personal data
  - Mitigation: Security awareness trainings to reduce the exposure of personal data

- **Service & Data Integration**
  - Risk: Proprietary data has to be protected as it is transferred between the end user and the cloud data center
  - Mitigation: Encryption (TLS, …)

OWASP Top 10 Cloud Security Issues (4)

- **Multi-tenancy & Physical Security**
  - Risk: Multi-tenancy usually means sharing of resources and services among multiple clients, depending on logical segregation to ensure that one tenant can not interfere with the security of the other tenants
  - Mitigation: Check out your cloud vendors offering for physical segregation

- **Incidence Analysis & Forensics**
  - Risk: In the event of a security incident, services hosted at a Cloud provider are difficult to investigate as logging may be distributed across multiple hosts and data centers
  - Mitigation: Check out your cloud vendor policy on handling and correlating event logs

OWASP Top 10 Cloud Security Issues (5)

- **Infrastructure Security**
  - Risk: All infrastructure must be hardened and configured securely
  - Mitigation: Configuration with tiering and security zones, role-based administrative access, regular risk assessments, policy for security updates, …

- **Non-production Environment Exposure**
  - Risk: Non-production (development, testing) environments are generally not secured to the same extent as the production environment
  - Mitigation: Avoid using real or sensitive data in non-production environments

OWASP Cloud-Native Application Security (1)

- **Insecure cloud, container or orchestration configuration**
  - Publicly open s3 bucket, container share resources with the host, insecure Infrastructure-as-Code (IaC) configuration, …
- **Injection flaws**
  - SQL injection, XML entity injection, serverless event data injection, …
- **Improper authentication & authorization**
  - Unauthenticated API access on a microservice, over-permissive cloud identity access management roles

https://owasp.org/www-project-cloud-native-application-security-top-10/

OWASP Cloud-Native Application Security (2)

- **CI/CD pipeline & software supply chain flaws**
  - Insufficient authentication on CI/CD pipeline systems, use of untrusted images, insecure communication channels to registries, …
- **Insecure secrets storage**
  - Orchestrator secrets stored unencrypted, API keys or passwords stored unencrypted inside containers or hardcoded, …
- **Over-permissive or insecure network policies**
  - Over-permissive pod to pod communication allowed, internal microservices exposed to the public Internet

OWASP Cloud-Native Application Security (3)

- **Using components with known vulnerabilities**
  - Vulnerable 3rd party open source packages, …
- **Improper assets management**
  - Undocumented microservices & APIs, obsolete cloud resources
- **Inadequate ‘compute’ resource quota limits**
  - Resource-unbound containers, over-permissive request quota on APIs
- **Ineffective logging & monitoring**

Thank you

Manfred Pamsl
T. +43/3862/33600-6305
manfred.pamsl@fh-joanneum.at