Cloud Fundamentals

Cloud-based technologies allow organizations to access computing, storage, software, and servers through the internet. This shifts the technological component of the organization to a cloud provider such as AWS, Azure, or Google Cloud.

Cloud Services

Software as a Service (SaaS)

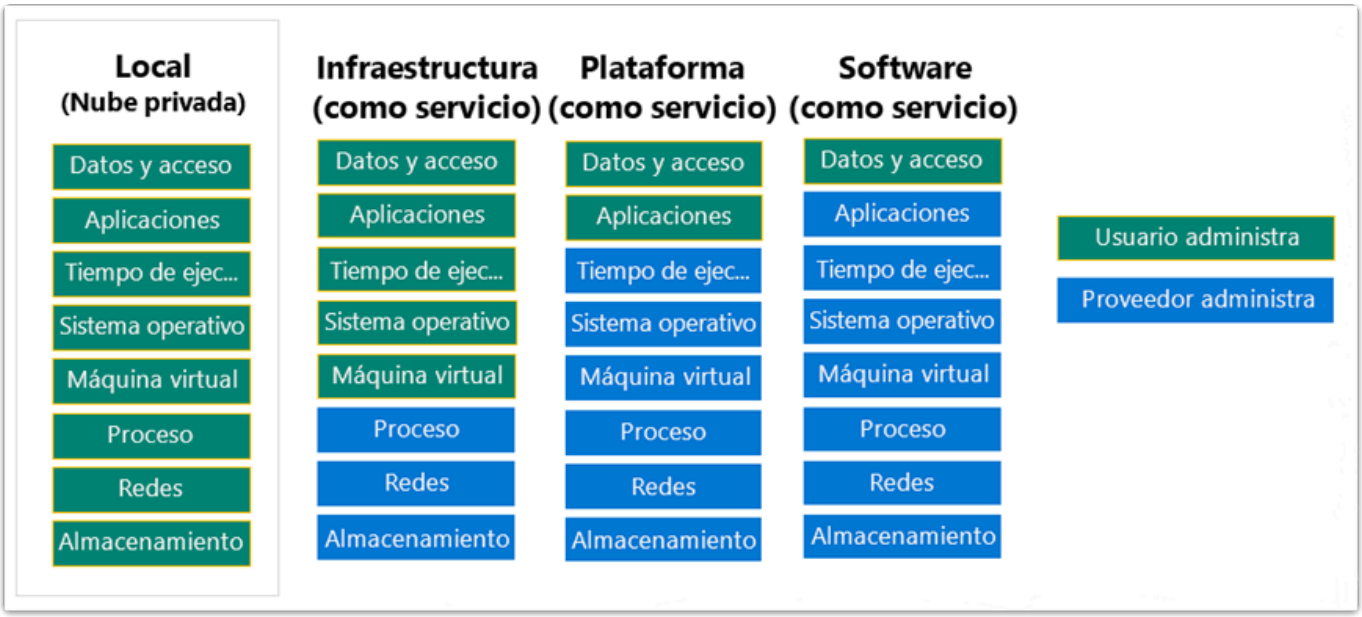
SaaS allows users to access applications and databases. Cloud providers manage the infrastructure while users store data on the cloud provider's servers.
Example: A user accesses Gmail, Google Drive, and Google Docs through Google Workspace without needing to install any software.

Platform as a Service (PaaS)

This enables an organization to remotely access development tools and services used to deliver applications through a subscription.
Example: A developer builds an application on Heroku without worrying about setting up servers or databases, as Heroku provides the necessary development tools and services.

Infrastructure as a Service (IaaS)

Provides virtualized computing resources over the internet. The provider hosts hardware, software, and storage components, while users pay for these resources flexibly, typically based on demand.
Example: A company rents AWS EC2 virtual instances to host its servers. The company installs the OS and applications, while AWS provides the virtualized hardware.



Types of Cloud

Cloud computing has different classifications based on the deployment method of service models.

Private Cloud

Also known as internal, corporate, or enterprise cloud, a private cloud is hosted on a private platform. It gives organizations more control over their data but can be more expensive due to infrastructure, maintenance, and management costs.
Example: A bank uses its own infrastructure to host critical systems like customer databases, ensuring full control over the data.

Public Cloud

Hosted by a service provider in an external facility. Users pay a monthly or annual subscription to access services. This option reduces infrastructure, maintenance, and management costs for the organization, but it also means less control over data.
Example: A startup uses Google Cloud services to store data and run applications, reducing infrastructure and maintenance costs.

Hybrid Cloud

Combines both private and public cloud, offering data control alongside the scalability of public cloud services.
Example: An online store stores confidential customer information on its private cloud but uses Microsoft Azure to scale during promotions or high-demand seasons.

Community Cloud

A collaborative effort where multiple organizations share and use the same platform, tailored to meet the needs of a specific sector like healthcare or energy.
Example: Several universities share a community cloud to store scientific research, optimizing resources and ensuring collaborative access.

Major Threats

Cloud computing is vulnerable to many threats that affect physical networks in any company. However, there are also unique threats, including:

Data Breach

Occurs when an unauthorized entity accesses protected confidential data.

Cloud Misconfiguration

Happens when cloud computing resources are improperly configured, making them vulnerable to attacks. Common examples include open storage permissions, unencrypted exposed databases, and lack of proper access control policies.

Poor Cloud Security Architecture Strategy

Since different cloud models have various security responsibilities, misunderstandings or improper implementation of cloud security architecture can lead to vulnerabilities.

Shared Account Credentials

This occurs when user accounts or access privileges are not well protected and are hijacked by attackers. This poses a significant security threat if the account has high-level privileges.

Insider Threat

Happens when an employee, contractor, or business partner compromises cloud service either maliciously or inadvertently.

Cloud Infrastructure Security

Company Security Policies

Well-defined company security policies and user training are effective ways to manage unknown applications.

Microsegmentation

Leverages virtual network topologies to run multiple, smaller, isolated networks without additional hardware costs. This technique enables more granular control of traffic security and workflows within the cloud.

Layered Security

Each cloud resource can be protected at multiple levels, such as:

- Hardware Layer: Use of secure devices in data centers.
- Infrastructure Layer: Proper configuration of virtual networks, firewalls, and VPNs.
- Platform Layer: Implementation of access controls for database services and runtime environments.
- Application Layer: Use of version control and software security testing mechanisms.

Cloud Application Security

Code Signing

Demonstrates that a piece of software is authentic. Executables designed for installation and execution on a device are digitally signed to validate the author's identity and ensure the software code has not been altered since signing.

Secure Cookies

Protects stored information from unauthorized access. Web developers should use cookies with HTTPS to secure them and prevent transmission over unencrypted HTTP.

Version Control

Prevents accidental changes made by authorized users. It ensures that two users cannot update the same object—like files, database records, or transactions—at exactly the same time.

Cloud Data Security

Cryptography

Encryption encodes data so that unauthorized people cannot easily read it. Unencrypted data is called plaintext, while the encrypted version is ciphertext.
There are two classes of encryption:

- Symmetric Encryption Algorithms: Use the same pre-shared key for encryption and decryption. They have a fixed block size of 128 bits with key sizes of 128, 192, or 256 bits.
- Asymmetric Encryption Algorithms: Use different keys for encryption and decryption. These include Rivest-Shamir-Adleman (RSA), Diffie-Hellman, ElGamal, and Elliptic Curve

Cryptography (ECC).

Hashing

Hashing ensures data integrity by taking binary data and producing a fixed-length representation called a hash value. These functions are one-way and used to verify data integrity and authentication.
Cryptographic hash functions have the following properties:

- Input can be of any length.
- Output has a fixed length.
- The hash function is one-way and irreversible.
- Two different input values almost never produce the same hash.
  The hash family includes:
- SHA-224 (224 bits)
- SHA-256 (256 bits)
- SHA-384 (384 bits)
- SHA-512 (512 bits)

Cloud Encryption Implementation

- In Transit: Uses TLS 1.2 or 1.3 to secure communication between client and server.
- At Rest: Automatic encryption of databases and storage using cloud provider-managed keys.
- In Use: Emerging techniques like homomorphic encryption (performs calculations directly on encrypted data without decrypting it, ensuring data privacy even during processing; while promising, it still faces performance challenges).