14th January 2025

1

Prof. Alessandro Carrega
alessandro.carrega@unige.it

Lesson 02

Introduction to Cloud Computing and Security

Ph.D. Course in Cyber Security for Cloud Computing
from zero to hero

What is Cloud Computing?

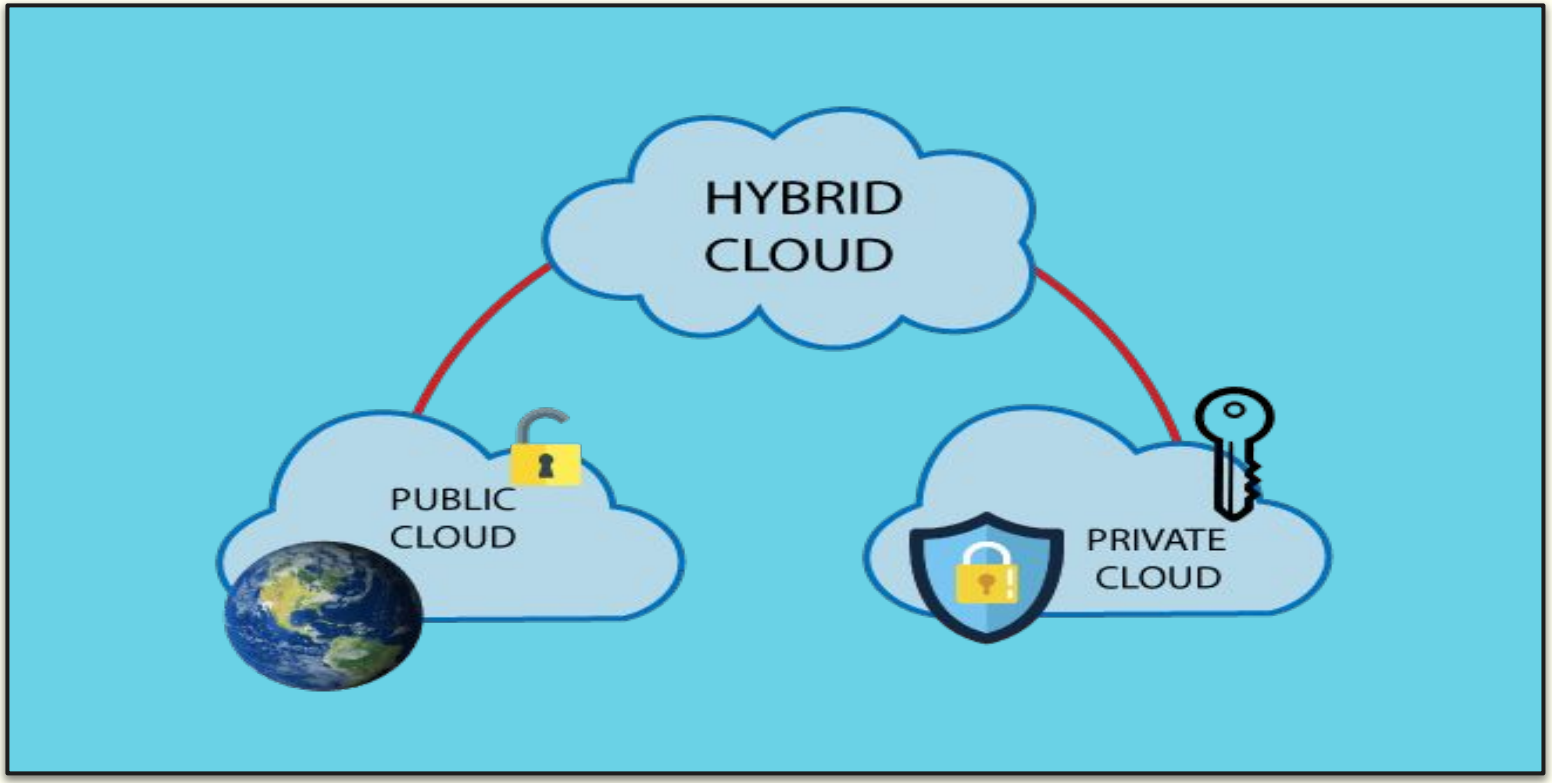
Cloud computing is the on-demand delivery of IT resources over the Internet with a pay-as-you-go pricing model

Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services such as computing power, storage, and databases on an as-needed basis from a cloud provider

Type of Cloud Computing

Public Cloud	*Private Cloud*	*Hybrid Cloud*
✖ Owned and operated by a third-party cloud service provider ✖ Resources are shared with multiple organizations ✖ *Example* Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)	✖ Dedicated cloud infrastructure for a single organization ✖ Can be on-premises or off-premises ✖ *Example* Self-managed data center	✖ Combines public and private clouds, allowing data and applications to be seamlessly moved between the two ones ✖ Provides flexibility and enhanced security

Type of Cloud Computing



Four Cloud Options

PRIVATE CLOUD

A private cloud is typically defined as everything behind a company's walls. These kinds of systems operate in a company's local data centers, although some companies prefer to use collocated data center facilities.

PUBLIC CLOUD

The public cloud includes a whole host of services and companies. The most common names are Microsoft Azure and AWS, among others. However, you may also hear software as a service such as Microsoft Office 365, included in the definition.

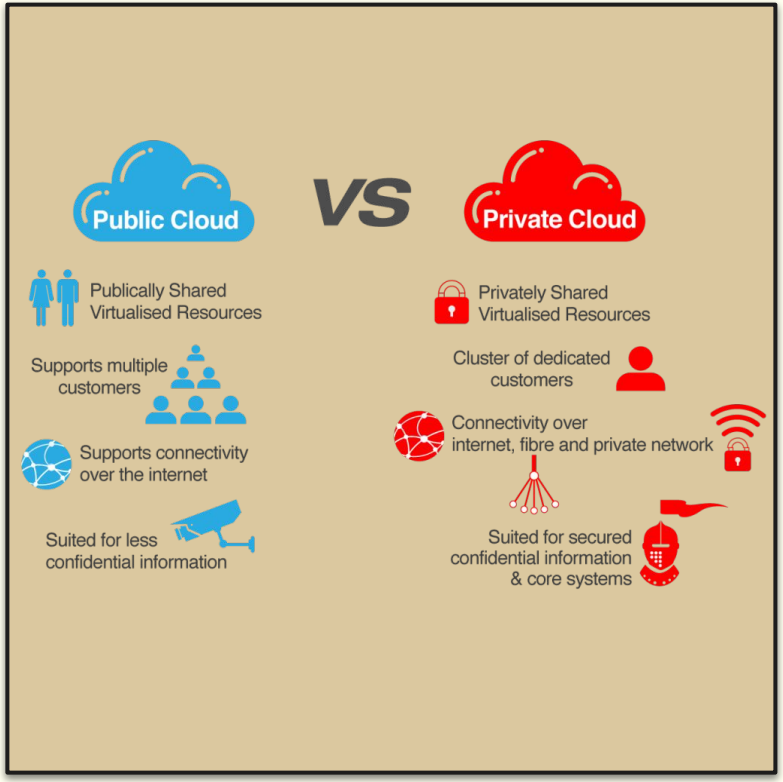
HYBRID CLOUD

A hybrid cloud deployment most typically describes a situation in which a company is operating both a private cloud and a public cloud. In general, in a hybrid cloud environment, the private and public services are integrated with one another.

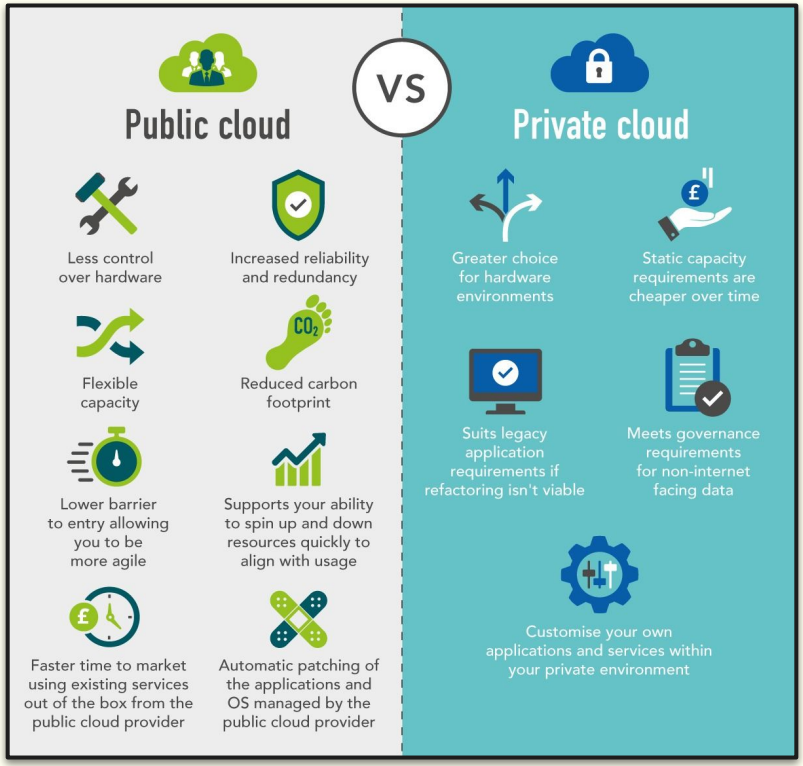
MULTI-CLOUD

A multi-cloud strategy is an approach that operates any combination of private, public, and hybrid clouds. An organization may have multiple public clouds and private clouds or multiple hybrid clouds, all either connected together or not.

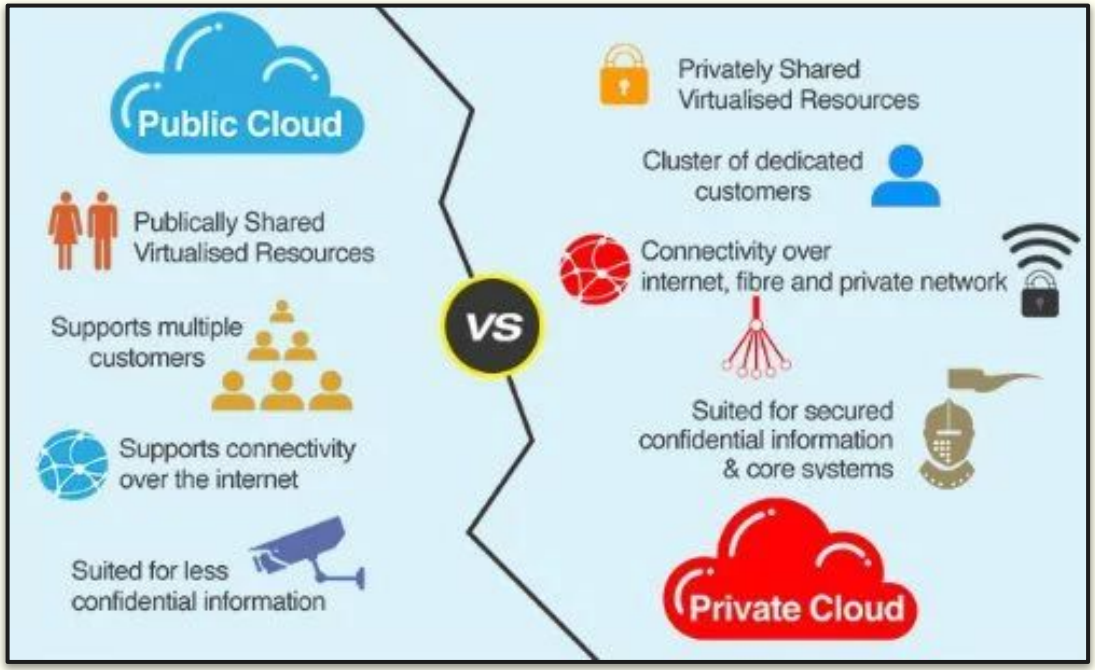
Public vs Private



Public vs Private



Public vs Private



Benefits of Cloud Computing

Cost-Effective pay only for the resources you use

Scalability easily scale resources up or down to meet changing demands

Reliability high availability and disaster recovery capabilities

Performance improved performance and faster innovation

Security robust security measures to protect data

Flexibility access resources from anywhere with an internet connection

The Shared Responsibility Model

A framework defining security responsibilities between a Cloud Service Provider (CSP) and its customers

It's a collaborative approach where both parties play crucial roles in ensuring the security of cloud environments

Cloud Service Provider's Responsibilities

Physical and Environmental Security	*Network and Infrastructure Security*	*System and Application Security*
✖ Securing data centers, hardware, and network infrastructure ✖ Implementing physical access controls, environmental controls, and disaster recovery plans	✖ Protecting the underlying network and infrastructure components ✖ Implementing firewalls, intrusion detection systems, and other security measures	✖ Ensuring the security of the cloud platform and underlying services ✖ Patching, updating, and securing operating systems and applications

Customer's Responsibilities

Customer Data	*Operating Systems, Applications, and Data*	*User Access and Identity Management*
✖ Protecting sensitive data stored and processed in the cloud ✖ Implementing encryption, access controls, and data loss prevention measures	✖ Securing operating systems, applications, and data deployed on cloud infrastructure ✖ Applying security patches, configuring firewalls, and implementing strong password policies	✖ Managing user identities and access privileges to cloud resources ✖ Implementing multi-factor authentication and role-based access control

Shared Responsibilities

Logging and Monitoring

- ✖ Both the CSP and customer share responsibility for logging and monitoring activities
- ✖ The CSP provides logging and monitoring tools, while the customer configures and analyzes logs

Incident Response

- ✖ Both parties collaborate on incident response planning and execution
- ✖ The CSP provides incident response capabilities, while the customer is responsible for incident detection and reporting

Understanding the Shared Responsibility Model Across Different Cloud Service Models

Infrastructure as a Service (IaaS)	*Platform as a Service (PaaS)*	*Software as a Service (SaaS)*
✖ Highest level of customer responsibility ✖ Customers manage operating systems, applications, and data	✖ Shared responsibility between CSP and customer ✖ CSP manages the platform, while customers manage applications and data	✖ Lowest level of customer responsibility ✖ CSP manages the entire application stack, including infrastructure, platform, and application

Remarks

The Shared Responsibility Model is essential for ensuring the security of cloud environments

By understanding the roles and responsibilities of both the CSP and customer, organizations can effectively mitigate risks and protect their data and applications

Collaboration and communication between the CSP and customer are key to successful implementation of the Shared Responsibility Model

Benefits of Cloud Computing

Stay informed keep up-to-date with the latest security best practices and threats

Leverage cloud provider security tools: utilize the security tools and services provided by your CSP

Regularly review and update security policies and procedures

Conduct security audits and penetration testing

Train employees on security awareness and best practices

Key Security Challenges

The Security Dilemma while the cloud offers immense advantages, it also introduces new security challenges

Challenge 1 – Data Breaches

Threat Landscape	*Cloud-Specific Vulnerabilities*	*Mitigation Strategies*
Increasing frequency and sophistication of data breaches	✖ Misconfigurations accidental exposure of sensitive data due to incorrect settings ✖ Weak Access Controls: inadequate authentication and authorization mechanisms ✖ *Insecure APIs* exploitable vulnerabilities in APIs	✖ *Implement strong access controls* multi-factor authentication, role-based access control ✖ Regular security audits and vulnerability assessments ✖ *Data encryption* protect data at rest and in transit ✖ *Incident response planning* develop a robust plan to respond to data breaches

Challenge 2 – Unauthorized Access

Insider Threats

Employees with malicious intent can compromise sensitive data

External Threats

Hackers and cybercriminals constantly seek vulnerabilities

Cloud-Specific Risks

- ✖ Weak password policies easily guessable passwords
- ✖ Phishing attacks tricking users into revealing credentials
- ✖ Social engineering manipulating users to gain unauthorized access

Mitigation Strategies

- ✖ Employee awareness training educate employees about security best practices
- ✖ Strong password policies enforce complex password requirements
- ✖ Intrusion detection and prevention systems monitor network traffic for suspicious activity
- ✖ Regular security audits and penetration testing

Challenge 3

DDoS Attacks	*Impact on Cloud Services*	*Mitigation Strategies*
Overwhelm systems with traffic, rendering them inaccessible	✖ Disrupted services impaired availability and performance ✖ Reputational damage negative impact on brand and customer trust ✖ Financial losses lost revenue and increased operational costs	✖ Robust DDoS protection solutions employ advanced mitigation techniques ✖ Network traffic filtering identify and block malicious traffic ✖ Cloud provider's security features leverage built-in DDoS protection capabilities ✖ Incident response plan to quickly mitigate the impact of DDoS attacks

Remarks

Importance of Proactive Security

Collaboration and Best Practices between cloud providers, security vendors, and organizations

Staying Informed encourage continuous learning and adaptation to evolving threats

The Need for Strong Network Security

The Digital Age

- ✖ Rapid digitization of information
- ✖ Increased reliance on technology
- ✖ Growing threat landscape

The Need for Strong Network Security

- ✖ Protecting sensitive data
- ✖ Maintaining business continuity
- ✖ Complying with regulations

Understanding the Threat Landscape

Cyber Threats

- ✖ Malware attacks
- ✖ Phishing scams
- ✖ Ransomware
- ✖ DDoS attacks
- ✖ Data breaches

The Rising Stakes

- ✖ Financial loss
- ✖ Reputation damage
- ✖ Legal repercussions

Data in Transit and at Rest

Data in Transit

- ✖ Data moving across networks
- ✖ Vulnerable to interception and manipulation

Data at Rest

- ✖ Data stored on devices and servers
- ✖ Target of unauthorized access and theft

Key Security Measures

Secure Access Control

- ✖ Implementing strong authentication and authorization
- ✖ Limiting access to sensitive data
- ✖ Regular Security Audits and Penetration Testing:
- ✖ Identifying vulnerabilities and weaknesses
- ✖ Implementing corrective measures

Firewalls

- ✖ Filtering network traffic
- ✖ Preventing unauthorized access

Encryption

- ✖ Converting data into unreadable code
- ✖ Protecting data both in transit and at rest

Intrusion Detection Systems (IDS)

- ✖ Monitoring network traffic for suspicious activity
- ✖ Detecting and alerting on potential threats

Regular Security Audits and Penetration Testing

- ✖ Identifying vulnerabilities and weaknesses
- ✖ Implementing corrective measures

Best Practices for Strong Network Security

Employee Training and Awareness

- ✖ Educating employees about security threats and best practices
- ✖ Promoting a security-conscious culture

Regular Patch Management

- ✖ Keeping software and systems up-to-date
- ✖ Addressing vulnerabilities promptly

Incident Response Plan

- ✖ Having a plan in place to respond to security incidents
- ✖ Minimizing damage and restoring operations

Data Backup and Recovery

- ✖ Protecting data from loss or corruption
- ✖ Enabling quick recovery in case of a breach

Remarks

The Importance of Proactive Security	*A Collaborative Approach*	*Safeguarding Your Digital Future*
✖ Investing in strong network security is essential ✖ Staying ahead of evolving threats	✖ Working with IT teams and security experts ✖ Implementing a layered security strategy	✖ Protecting your organization's valuable assets ✖ Building a resilient and secure digital infrastructure

The Importance of a Robust Security Strategy

In today's digital age, the cloud has become an indispensable tool for businesses of all sizes

It offers scalability, flexibility, and cost-effectiveness, enabling organizations to innovate and grow at an unprecedented pace

However, with these benefits comes a new set of challenges, particularly in the realm of security

As more and more sensitive data migrates to the cloud, the need for a robust security strategy becomes paramount

Understanding the Cloud Security Landscape

Shared Responsibility Model	*Common Cloud Security Threats*	*Denial-of-service (DoS) attacks*
• Cloud providers are responsible for securing the infrastructure ✖ Organizations are responsible for securing their data and applications	✖ Data breaches ✖ Malware attacks	✖ Misconfigurations ✖ Insider threats

Building a Secure Cloud Foundation

Strong Identity and Access Management (IAM)

- implement strong password policies and multi-factor authentication (MFA).
- Grant least privilege access to resources.
- Regularly review and revoke access permissions.

Data Encryption

- Encrypt data both at rest and in transit.
- Use industry-standard encryption algorithms.

Network Security

- Utilize firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- Segment networks to limit the impact of potential breaches.

Regular Security Assessments

- Conduct regular vulnerability assessments and penetration testing.
- Stay updated on the latest security threats and patches.

Incident Response Plan

- Develop a comprehensive incident response plan.
- Test the plan regularly to ensure its effectiveness.

Employee Training and Awareness

- Educate employees about security best practices.
- Conduct regular security awareness training.

Best Practices for Secure Cloud Environment

Choose a Reputable Cloud Provider select a provider with a strong security track record

Stay Updated with Security Patches regularly apply security patches to your cloud infrastructure

Monitor and Log Activity continuously monitor your cloud environment for suspicious activity.

Implement Security Automation automate security tasks to improve efficiency and reduce human error.

Collaborate with Security Experts seek expert advice to strengthen your security posture.

Remarks

By adopting a proactive and comprehensive security strategy, organizations can mitigate risks and protect their valuable assets in the cloud

A secure cloud foundation is essential for building trust with customers and partners.

Remember, security is not an afterthought; it should be an integral part of your cloud journey from the very beginning

End of Lesson

Q/A