

Cloud Computing e la Sicurezza?

Virtualizzazione e Sicurezza ICT

Diego Feruglio

Direzione Tecnica
Area Ricerca Applicata

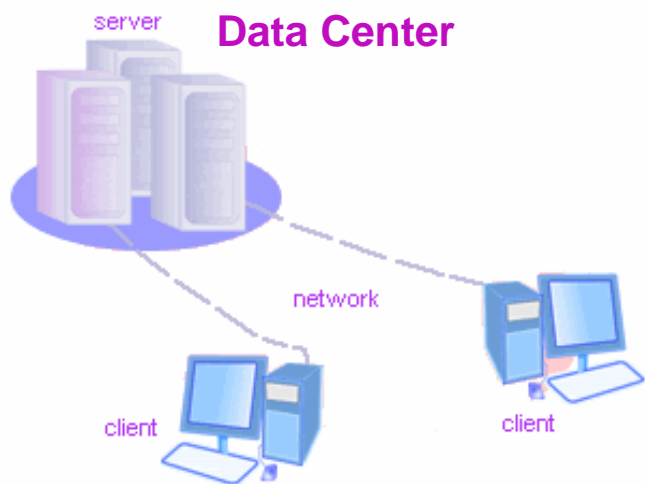
Cloud Computing e la sicurezza?

Definizione e tassonomia

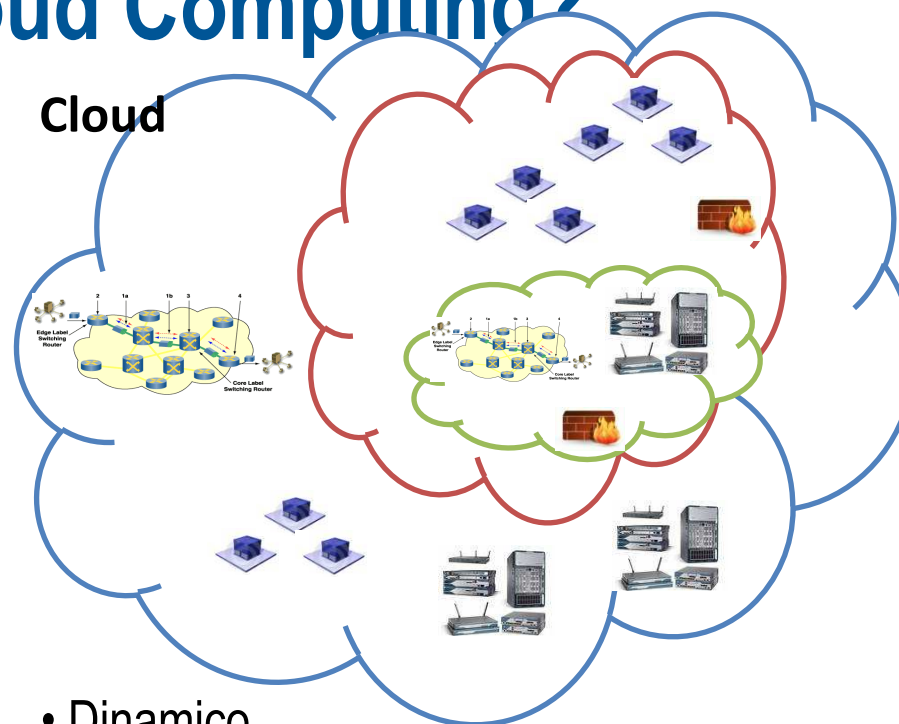
Il Cloud Computing



Cosa si intende per Cloud Computing?



- Progettato per essere statico
- Risorse rigide
- Processi di provisioning manuale
- Limitato dalla rete



- Dinamico
- Infrastruttura condivisa
- Automatizzato/elastico
- Scalabile
- Pay per use
- Multi-tenant

Cloud Computing: definition by NIST

Cloud Computing: 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. (This definition is from the latest draft of the **NIST Working Definition of Cloud Computing** published by the U.S. Government's **National Institute of Standards and Technology**)

Delivery Models

The **NIST** definition of cloud computing defines three delivery models:

Software as a Service (SaaS): The **consumer uses an application**, but does not control the operating system, hardware or network infrastructure on which it's running.

Platform as a Service (PaaS): The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an **application framework**.

Infrastructure as a Service (IaaS): The consumer uses "fundamental computing resources" such as processing power, storage, networking components or **middleware**. The consumer can control the operating system, storage, deployed applications and possibly networking

Cloud Computing: definition by NIST

The **NIST definition** defines four deployment models:

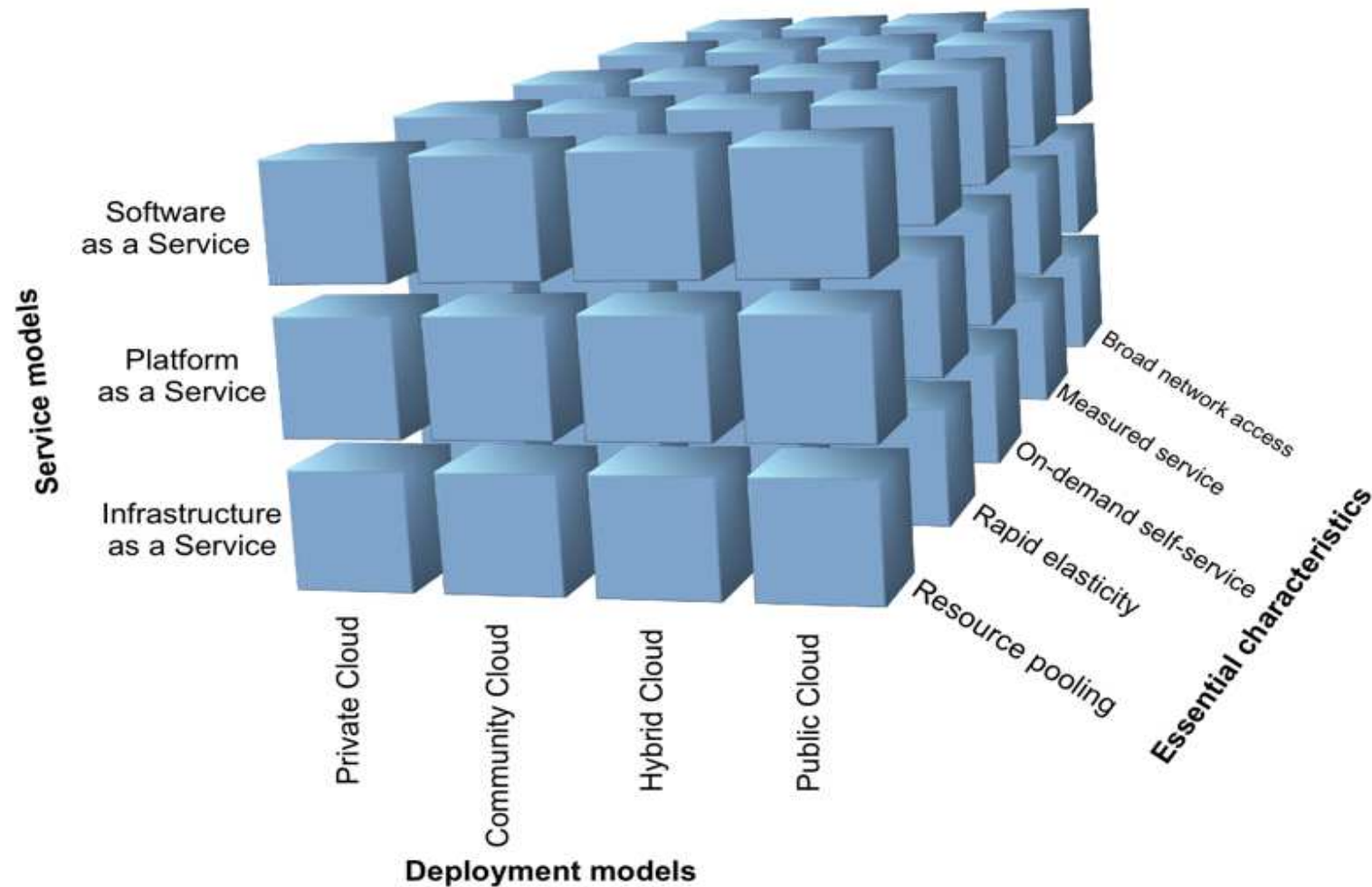
Public Cloud: In simple terms, public cloud services are characterized as **being available to clients from a third party service provider via the Internet**. The term “public” does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user’s data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.

Private Cloud: A private cloud offers many of the benefits of a public cloud computing environment, such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, **data and processes are managed within the organization** without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

Community Cloud: A community cloud is controlled and used by a **group of organizations that have shared interests**, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

Hybrid Cloud: A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically **outsource nonbusiness-critical information and processing to the public cloud**, while keeping business-critical services and data in their control.

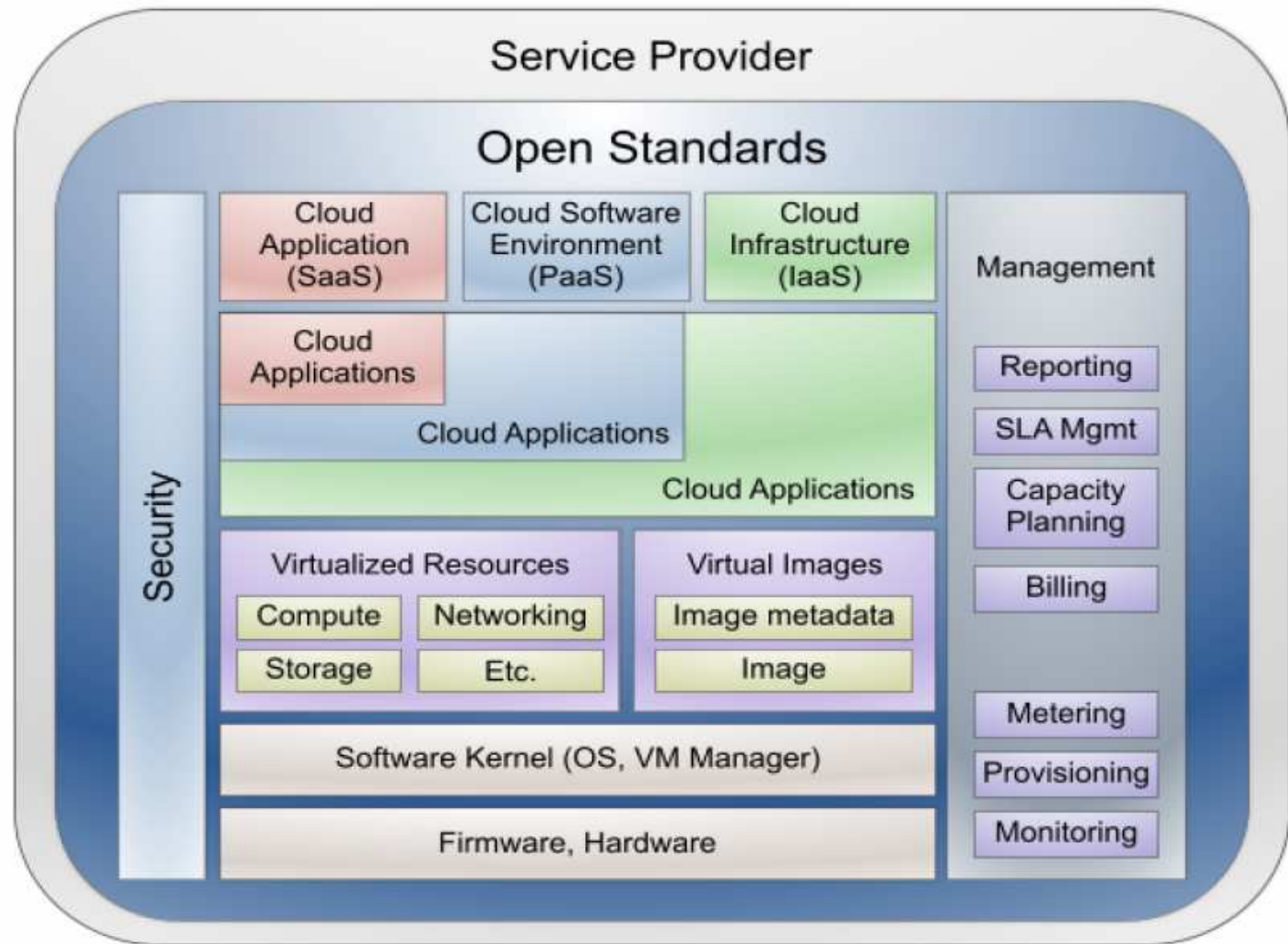
Cloud Computing: definition by NIST



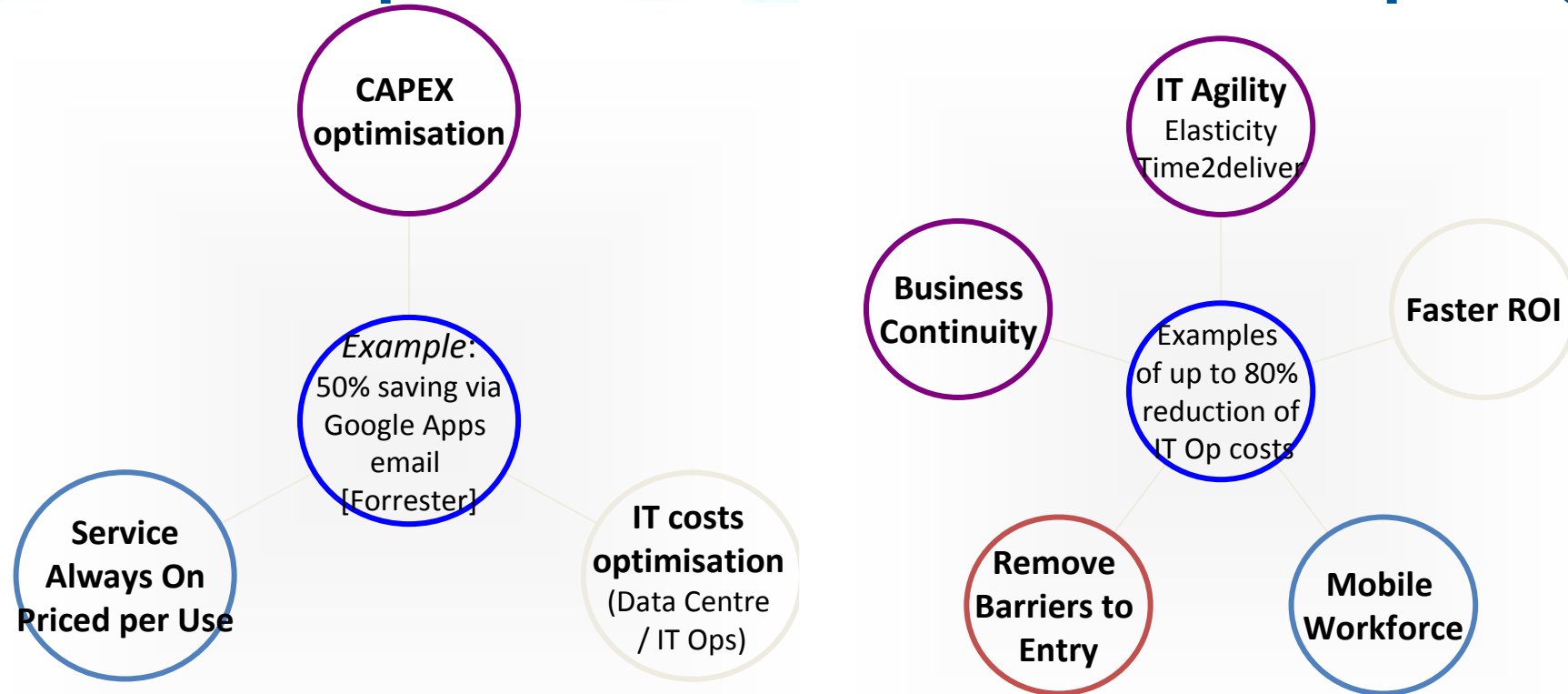
Tassonomia

Cloud Computing
Use Cases
White paper 3.0

Open Cloud Manifesto



Motivazioni per l'adozione del Cloud Computing



Chief
Financial
Officer's view 

Chief
Operating
Officer's view 

Cloud Computing e la sicurezza?

I rischi

Rischi per scenari di Cloud Computing

.IaaS:

- Le Virtual Machines (VM) sono vulnerabili
- Le VM propagano i rischi
- Le VM utilizzano in modo eccessivo le risorse di calcolo e di rete
- Utilizzo di INTERNET che è «untrusted» per definizione
- Session Hijacking

Esempi:

Abuso dell'infrastruttura Cloud
Insicura/obsoleta crittografia
Insufficiente controllo rete
virtualizzata
Web services vulnerabili
Problemi da Shared
Technology
Perdita dei dati

.Indicatori di rete:

- «Malicious traffic» transita verso la rete
- Eccessivo e non previsto traffico generato da applicazioni malevole

Rischi per scenari di Cloud Computing

- PaaS
 - Piattaforme di sviluppo vulnerabili
 - Nel «multitenant» le separazioni tra i contesti non sono rinforzabili e monitorate
 - Malicious code può impattare nel dominio del vicino
 - Utilizzo di INTERNET che è «untrusted» per definizione
- Indicatori di rete:
 - Tentativi di forzatura possono essere scoperti da controlli sul traffico
 - Malicious code può essere scoperto da controlli sul traffico
 - Eccessivo e non previsto traffico generato da applicazioni malevole

Esempi:

Abuso dell'infrastruttura Cloud
Insicura/obsoleta crittografia
SQL injection
Perdita dei dati
Hijacking degli account

Rischi per scenari di Cloud Computing

- SaaS
 - Il software è vulnerabile
 - Il software è eseguito una sola volta per molti clienti
 - Il singolo «sw context exploitation» impatta su clienti multipli
 - Utilizzo di INTERNET che è «untrusted» per definizione
- Indicatori di rete:
 - Malicious traffic può essere rivelato da gruppi di pacchetti segnati
 - Tentativi di intrusione possono essere encriptati ma l'eccesso di tentativi può essere scoperto

Esempi:
Insicura/obsoleta crittografia
Codice per il controllo autorizzativo insufficiente o con fault
Perdita dei dati
Hijacking degli account

Cloud Computing: laboratorio

- In CSI-Piemonte è attivo dal 2008 un laboratorio focalizzato sul Cloud Computing con l'obiettivo di:
 - Valutare i modelli di cloud
 - Effettuare sperimentazioni
 - Acquisire esperienze per evitare problemi nell'adozione del cloud
 - Valutare l'evoluzione dell'infrastruttura secondo questo modello

Cloud Security: riferimenti

- Cloud Security Alliance (CSA)
<http://www.cloudsecurityalliance.org/>
 - Guida sui rischi del Cloud
 - Guida su Identity e Access Management
- CIO.GOV <http://www.cio.gov/>
 - Documento di indicazione sui rischi per l'utilizzo del Cloud in ambiente "government"



Grazie

Diego Feruglio
Direzione Tecnica
Area Ricerca Applicata