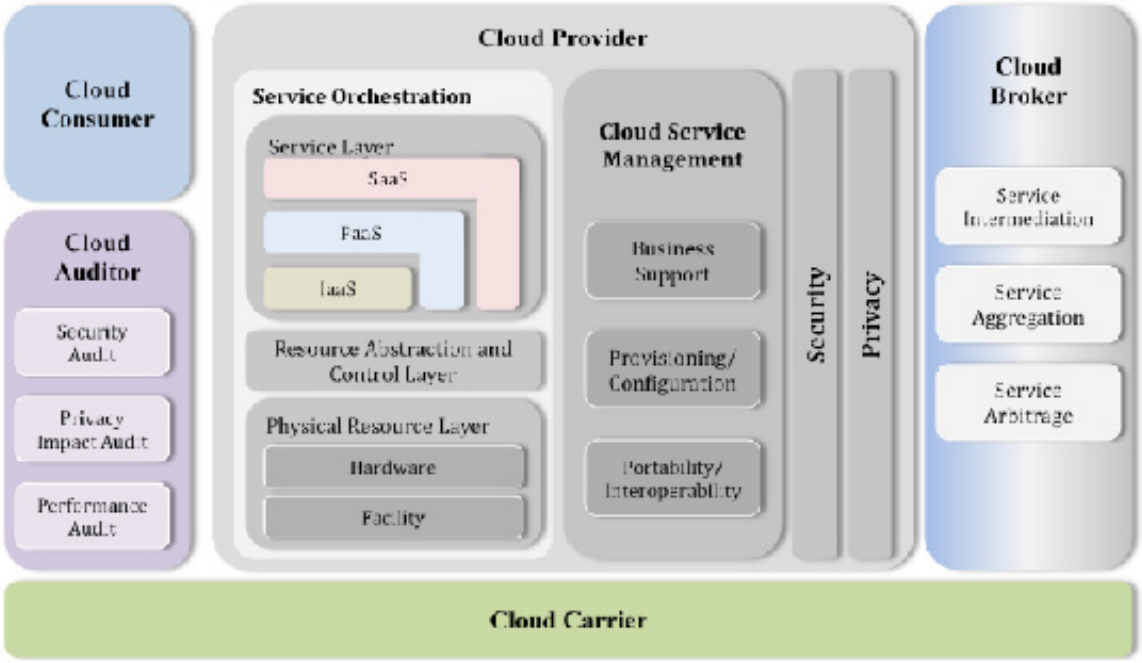
CLOUD COMPUTING REFERENCE ARCHITECTURE: LE INDICAZIONI DEL NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Nella newsletter N°4 abbiamo già parlato di Cloud Computing, introducendone i concetti allo scopo di condividere i modelli operativi ed avviare una discussione su cosa cambia dal punto di vista dell'IT Governance; vogliamo ora riprendere l'argomento cogliendo un'occasione fornita dal NIST, il *National Institute for Standards and Technology*, l'agenzia federale del dipartimento del commercio americano.

Il NIST ha pubblicato, lo scorso settembre 2011, il documento "NIST Cloud Computing Reference Architecture", che definisce un'architettura di riferimento (Cloud Computing Reference Architecture – CCRA) ed una tassonomia che aiuti a classificare i componenti e le tipologie di offerta. Il lavoro ha l'obiettivo di contribuire ad accelerare l'adozione, da parte del governo degli Stati Uniti, di servizi basati su standard sicuri di cloud computing al fine di ridurre i costi e migliorare i servizi.
L'articolo, basato su uno studio autorevole, è molto utile a consolidare alcuni concetti e a stabilire un vocabolario comune su uno degli argomenti più chiacchierati del momento.
Lo studio, focalizzato su cosa i servizi cloud forniscono piuttosto che come sono realizzati, è articolato in due parti: la prima parte è una panoramica sui principali attori e i loro rispettivi ruoli, la seconda parte descrive i componenti del servizio e la loro "orchestrazione"; in questo articolo ne riportiamo una sintesi.

Prima parte: Panoramica sugli attori

Con il diagramma che segue, che identifica i principali attori e le rispettive funzioni, il NIST rappresenta un'architettura di alto livello intesa a facilitare i requisiti, gli usi, le caratteristiche e gli standard del *Cloud Computing*:



(fonte immagini: NIST Cloud Computing Reference Architecture - Special Publication 500-292)

Come si vede, sono definiti cinque principali attori: il *cloud consumer*, il *cloud provider*, il *cloud carrier*, il *cloud auditor*, il *cloud broker*.

La tabella che segue, tradotta dall'articolo originale del NIST, descrive brevemente le funzioni dei cinque attori:

Attore	Definizione
Cloud Consumer	Persona od organizzazione che ha una relazione di business con, ed usa i servizi di, uno o più Cloud Provider.
Cloud Provider	Persona, organizzazione o entità responsabile di rendere il servizio disponibile alle parti interessate.
Cloud Auditor	Terza parte che possa condurre una verifica dei servizi, dell'esercizio dei sistemi informativi, delle prestazioni e della sicurezza della implementazione cloud.
Cloud Broker	Entità che gestisce l'uso, le prestazioni e l'erogazione dei servizi cloud e negozia le relazioni tra i Cloud Provider e i Cloud Consumer.
Cloud Carrier	Intermediario che fornisce la connettività e il trasporto dei servizi cloud dai Cloud Provider ai Cloud Consumer.

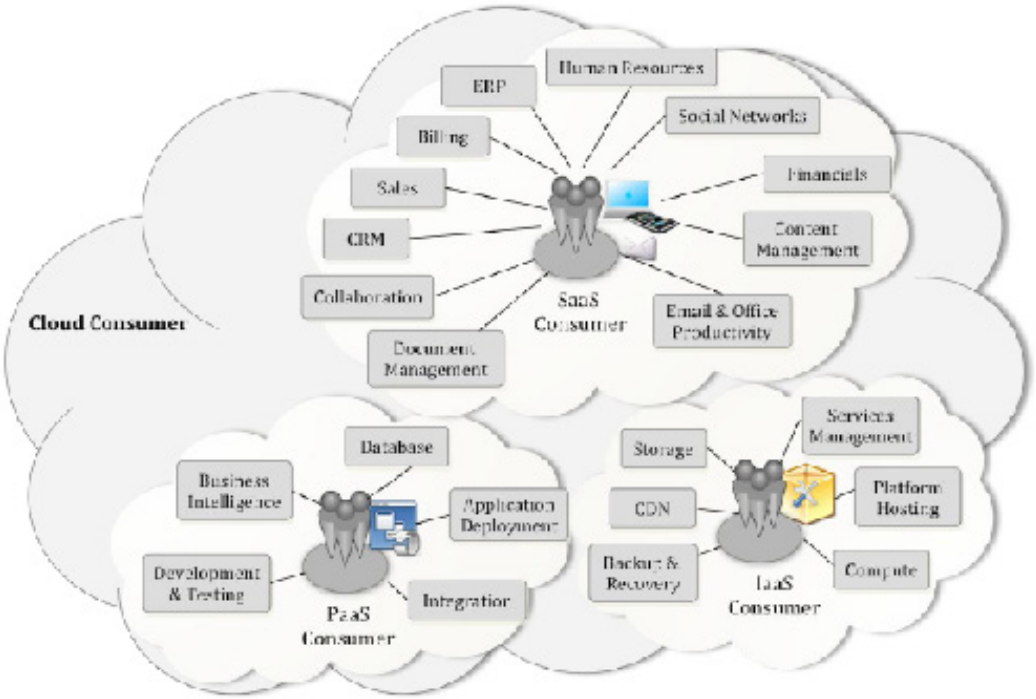
Lo studio, prima di approfondire le funzioni e prerogative di ciascuno degli attori identificati, espone tre scenari di interazione tra gli attori (schemi presida NIST Cloud Computing Reference Architecture - Special Publication 500-292):

Scenario 1: un Cloud Consumer richiede servizi a un Cloud Broker piuttosto che direttamente al Cloud Provider. Il Cloud Broker crea un nuovo servizio combinando servizi di più provider e/o ampliando i servizi esistenti:

Scenario 2: un Cloud Provider definisce due accordi sui livelli di servizio (SLA), uno con il Cloud Carrier ed uno con il Cloud Consumer:

Scenario 3: un Cloud Auditor conduce verifiche indipendenti sulle operazioni e la sicurezza della implementazione Cloud. L'audit può coinvolgere interazioni sia con il Cloud Consumer che con il Cloud Provider:

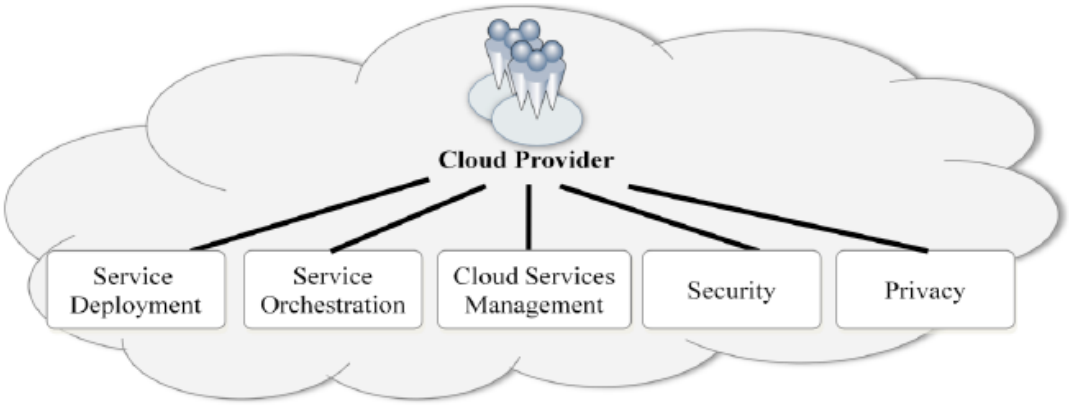
L'articolo prosegue con una descrizione più estesa delle categorie di attori.
Per quanto riguarda i ***Cloud Consumer***, riprendiamo una figura dall'articolo originale che rappresenta l'universo dei consumer nell'ambito delle tre tipologie di servizi Cloud, IaaS (*infrastructure as a Service*), PaaS (*Platform as a Service*), SaaS (*Software as a Service*):



Per la categoria dei **Cloud Provider**, l'articolo sintetizza le funzioni dell'attore nell'ambito delle tre categorie di servizi Cloud:

- **SaaS**: il provider dispiega, configura, manutiene e aggiorna le applicazioni software in conformità ai livelli di servizio concordati con il consumer. Il consumer ha, in questo caso, un limitato controllo amministrativo sulle applicazioni.
- **PaaS**: il provider gestisce l'infrastruttura e i componenti della piattaforma (come database, middleware,…) e supporta i processi di sviluppo del consumer con strumenti tipo IDE, SDK, etc. Il consumer ha, in questo caso, il controllo sulle applicazioni e su alcuni parametri ambientali, ma nessuno o limitato accesso alle infrastrutture sottostanti.
- **IaaS**: il provider gestisce le risorse fisiche dell'infrastruttura, inclusi i server, le reti e lo storage. Il consumer usa le risorse messe a disposizione dal provider e, rispetto ai consumer di servizi PaaS o SaaS, ha accesso e maggiore controllo sull'infrastruttura di sistema.

Il NIST sintetizza le attività del Provider nelle cinque aree rappresentate nella figura seguente:



Nell'articolo del NIST l'attore **Cloud Broker** è riferito a tre categorie di servizi:

- **Service Intermediation**: il broker fornisce servizi a valore aggiunto rispetto ai provider; esempi possono essere: accesso ai servizi, identity management, reporting, sicurezza addizionale, etc.
- **Service Aggregation**: il broker combina ed integra servizi di più provider in uno o più nuovi servizi.
- **Service Arbitrage**: simile al Service Aggregation, ad eccezione del fatto che i servizi aggregati non sono fissi. Il broker ha, in questo caso, la flessibilità di scegliere tra diversi provider ed agenzie sulla base di criteri di selezione dei migliori.

Nell'articolo, il NIST riporta una chiara schematizzazione dell'integrazione del controllo tra Provider e Consumer sulle risorse in Cloud in funzione del tipo di servizio:

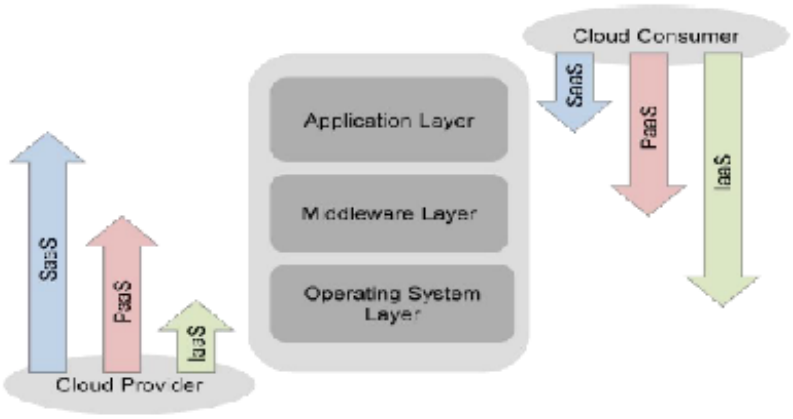
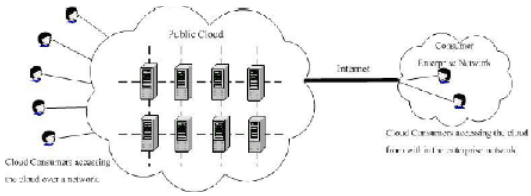


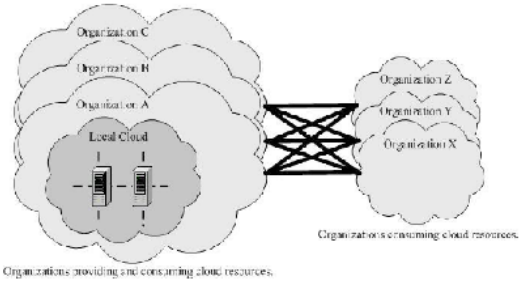
Figure 8: Scope of Controls between Provider and Consumer

Seconda parte: Componenti architetturali

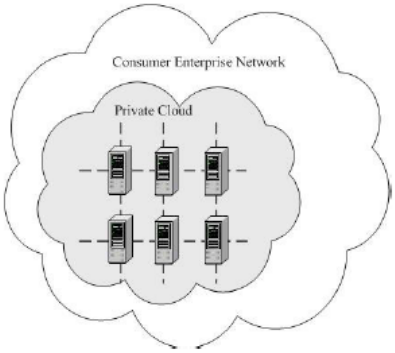
La seconda parte dell'articolo del NIST inizia con una disamina dei modelli di esercizio di un'infrastruttura Cloud: ***Public Cloud***, ***Private Cloud***, ***Community Cloud***, ***Hybrid Cloud***. Le differenze riguardano il livello di esclusività con cui le risorse sono erogate al consumer.



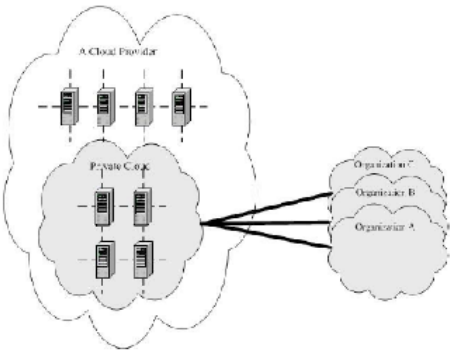
Public Cloud



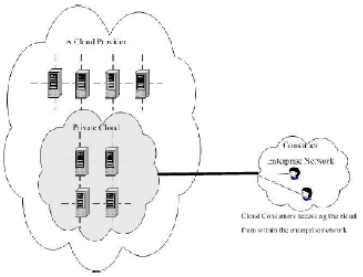
On-site Community Cloud



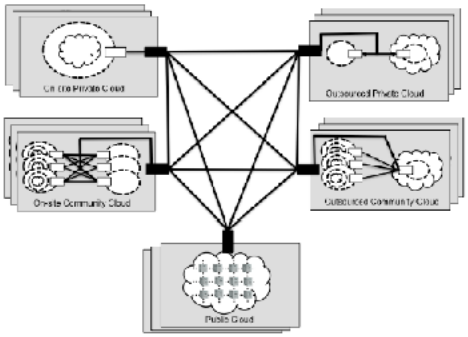
On-site Private Cloud



Outsourced Private Cloud

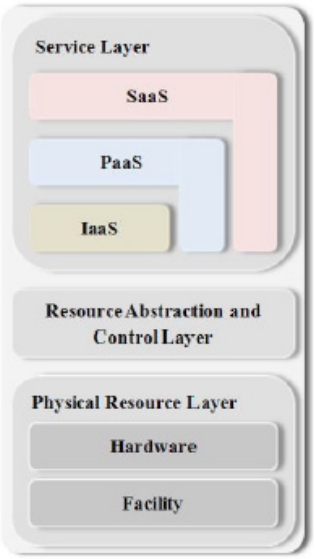


Outsourced Community Cloud



Hybrid Cloud

Dopo la descrizione dei modelli di esercizio, l'articolo del NIST si sofferma sulla funzione di **Service Orchestration** o, in altre parole, di selezione, integrazione, coordinamento e gestione delle risorse necessarie all'erogazione dei servizi richiesti dal consumer.I componenti sono raggruppati in tre layer: **Service Layer, Resource Abstraction and Control Layer, Physical Resource Layer:**

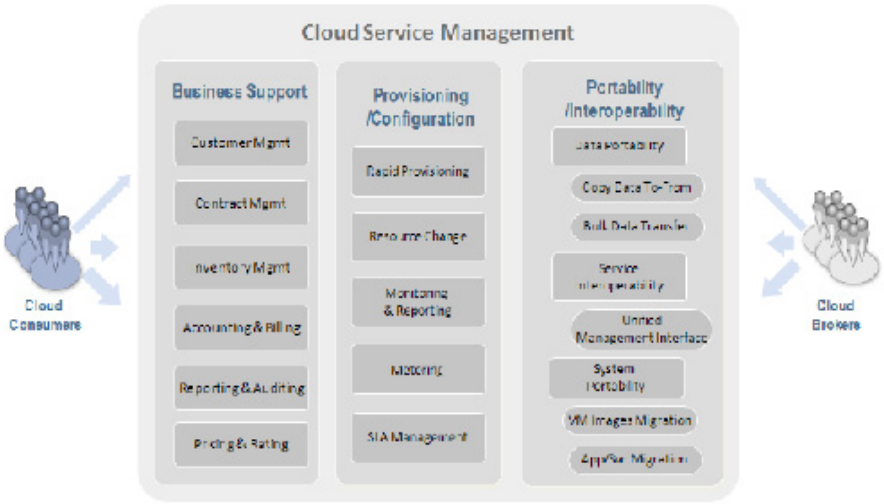


Il **Service Layer** è l'area dove il provider definisce le interfacce per l'accesso dei consumer ai servizi.

Il **Resource Abstraction and Control Layer** contiene i componenti che il provider usa per fornire e gestire l'accesso alle risorse fisiche di elaborazione attraverso un'astrazione del software. Esempi di componenti di astrazione sono elementi quali: hypervisor, macchine virtuali, sistemi di storage virtuale.

Il **Physical Resource Layer**, il più basso, include tutte le risorse fisiche. Sono quindi inclusi: computer (CPU e memoria, etc.), componenti di rete (router, switch, bilanciatori, firewall, interfacce, etc.), componenti di storage, infrastrutture di facility (sale dati, HVAC, sistemi di alimentazione, etc.)

Un altro componente importante, secondo il NIST, è l'insieme – ***Cloud Service Management*** - delle funzioni necessarie per la gestione e l'esercizio dei servizi:



Il Cloud Service Management è quindi articolato nelle tre componenti rappresentate nella figura e descritte più estesamente nell'articolo:

- **Business Support**
- **Provisioning / Configuration**
- **Portability / Interoperability**

Gli ultimi due componenti presi in considerazione dal NIST sono la Sicurezza (Security) e la Privacy:

- A proposito della sicurezza, il NIST sottolinea come sia un elemento che si estende a tutti i livelli del modello dal fisico all'applicativo, imponendo l'indirizzamento dei requisiti di sicurezza come l'autenticazione, l'autorizzazione, la disponibilità, la confidenzialità, la gestione delle identità, l'integrità, l'audit, il monitoraggio, la risposta agli incidenti, la gestione delle policy di sicurezza. Alcuni accenti vengono posti sulla importanza di determinare, per le diverse tipologie di servizio e relative implementazioni, gli impatti sul business e le diverse problematiche in fase di progettazione e realizzazione. Ad esempio, vengono citati i requisiti di sicurezza dell'accesso via browser ai servizi SaaS o ai requisiti di isolamento delle Virtual Machine nei servizi IaaS.
  Evidentemente, le implicazioni di sicurezza sono molto diverse anche in funzione dei modelli di esercizio attuati (Public Cloud, Private Cloud, Outsourced Cloud, etc.).
  Un elemento molto importante messo in evidenza dall'articolo è che la sicurezza è sempre una responsabilità condivisa tra consumer e provider, con confini sempre diversi a seconda del tipo di servizio. I controlli da attuare devono essere adeguatamente analizzati al fine di determinare quale delle parti è nella migliore condizione per implementarli. Nell'articolo si fa l'esempio dei controlli di gestione degli account che, in uno scenario IaaS, sono attuati dal provider per la configurazione iniziale degli utenti privilegiati, ma per la gestione delle applicazioni restano di responsabilità del consumer.
- Per quanto riguarda la Privacy, l'articolo sottolinea come i servizi in Cloud, pur fornendo nuove e flessibili soluzioni per l'uso di risorse condivise, introducano nuovi rischi e pongano nuove sfide per assicurare le necessarie garanzie di protezione dei dati personali degli utenti.

L'articolo si conclude con la tassonomia del Cloud; la tassonomia è presentata con uno schema a quattro livelli:

- **Level 1: Ruoli**
- **Level 2: Attività**
- **Level 3: Componenti**
- **Level 4: Sub-componenti**

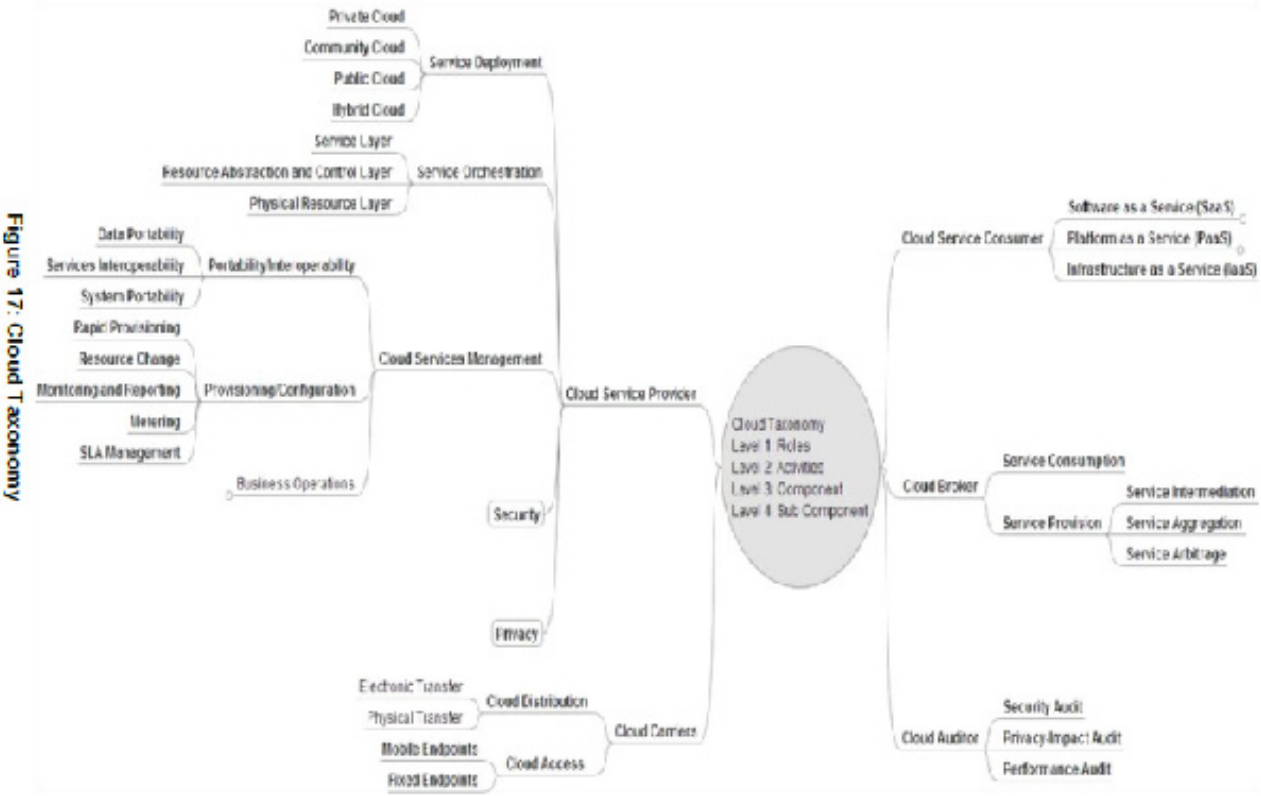


Figure 17: Cloud Taxonomy

Nelle appendici all'articolo sono, inoltre, riportati:

- un glossario dei termini e delle definizioni utilizzati nella tassonomia
- alcuni esempi di servizi cloud
- un interessante bibliografia che riporta i riferimenti utilizzati per l'articolo

HSPI SpA - Consulenti di Direzione
Viale Aldo Moro 16 - 40127 Bologna (Italy)
P.IVA 02355801206

Tel. +39 051 2960545 | Fax. +39 051 6568695
BOLOGNA | MILANO | ROMA
www.hspi.it | e-mail: info@hspi.it