IL CLOUD

STRUTTURA E SICUREZZA

Dalle moderne generazioni alle grandi aziende, tutti fanno ricorso, seppur inconsapevolmente, al CLOUD.
Quasi certamente, tutti i giorni abbiamo a che fare con il cloud: Office 365, il 5G che sarà fornito dagli operatori telefonici, Amazon Web Service (https://aws.amazon.com/) che include Amazon Elastic compute cloud (EC2), in tutti questi casi utilizziamo il cloud; lo troviamo nei servizi di storage forniti da Google Drive (https://gsuite.google.com/intl/en_ie/), in Dropbox (https://www.dropbox.com/) e non per ultima, la nostra posta elettronica non è altro che un software as a service (SaaS).
Per cui, la necessità di tutti, aziende comprese, di archiviare, condividere, rendere fruibili una enorme quantità di dati, ha reso il cloud un elemento essenziale.

Ok, ma cos'è il Cloud computing?Come è caratterizzato?
Il Nist, National Institute of Standard and Technology, nella sua Special Publication 800-145 ha definito il cloud computing e le sue caratteristiche:

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.

"Il cloud computing è un modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi".

Dunque, è la possibilità di usufruire, da parte di un utente(privato/azienda), di risorse computazionali on demand, disponibili, di facile accesso e rilascio.

La stessa definizione anticipa alcune delle caratteristiche del cloud, ma vediamole nel dettaglio:

- *Self-service su richiesta.*Un consumatore può acquisire, unilateralmente e automaticamente, le necessarie capacità di calcolo, come tempo macchina e memoria, senza richiedere interazione umana con i fornitori di servizi.
- *Accesso in rete a larga banda.*Le capacità sono disponibili in rete e accessibili attraverso meccanismi standard che promuovono l'uso attraverso piattaforme eterogenee come client leggeri o pesanti (ad esempio telefoni mobili, tablet, laptops e workstations).
- *Condivisione delle risorse.* Le risorse di calcolo del fornitore sono messe in comune per servire molteplici consumatori, utilizzando un modello condiviso (multi-tenant) con le diverse risorse fisiche e virtuali, assegnate e riassegnate dinamicamente in base alla domanda. Dato il senso di indipendenza dalla locazione fisica, l'utente generalmente non ha controllo o conoscenza dell'esatta ubicazione delle risorse fornite, ma può essere in grado di specificare la posizione ad un livello superiore di astrazione (ad esempio, paese, stato o data center). Esempi di risorse includono memoria, elaborazione e larghezza di banda della rete.

- *Elasticità rapida.*Le risorse possono essere acquisite e rilasciate elasticamente, in alcuni casi anche automaticamente, per scalare rapidamente in relazione alla domanda. Al consumatore, le risorse disponibili spesso appaiono illimitate e disponibili in qualsiasi quantità, in qualsiasi momento.
- *Servizio misurato*.I sistemi cloud controllano automaticamente e ottimizzano l'uso delle risorse, facendo leva sulla capacità di misurazione ad un livello di astrazione appropriato per il tipo di servizio (ad esempio memoria, elaborazione, larghezza di banda e utenti attivi). L'utilizzo delle risorse può essere monitorato, controllato e segnalato, fornendo trasparenza sia per il fornitore che per l'utilizzatore del servizio.

Tali caratteristiche risultano integrate nei diversi modelli di servizio individuati dal NIST,

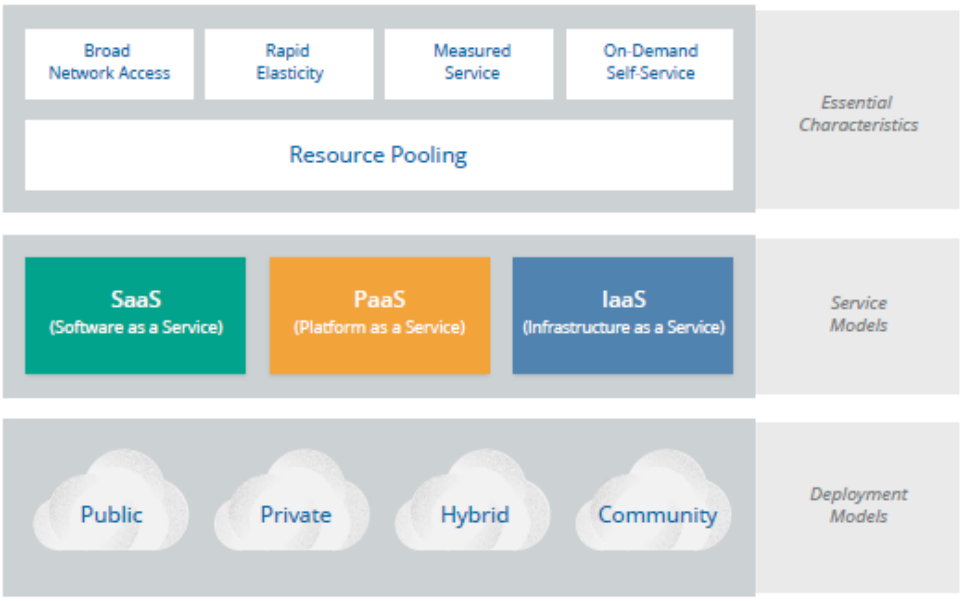

Figura 1. Caratteristiche e modelli.

- ***Software as a Service - SaaS.***
  - Al consumatore viene fornita la facoltà di utilizzare le applicazioni del fornitore, funzionanti su un'infrastruttura cloud. Le applicazioni sono accessibili da diversi dispositivi attraverso un'interfaccia leggera (thin client), come ad esempio un'applicazione email su browser, oppure da programmi dotati di apposita interfaccia. Il consumatore non gestisce o controlla l'infrastruttura cloud sottostante, compresi rete, server, sistemi operativi, memoria, e nemmeno le capacità delle singole applicazioni, con la possibile eccezione di limitate configurazioni a lui destinate (parametrizzazione).

- ***Platform as a Service – PaaS.***
  - Il consumatore ha facoltà di distribuire, sull'infrastruttura cloud, applicazioni create in proprio o acquisite da terzi, utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il consumatore non gestisce ne controlla l'infrastruttura cloud sottostante, compresi rete, server, sistemi operativi, memoria, ma ha il controllo sulle applicazioni ed eventualmente sulle configurazioni dell'ambiente che le ospita.

- ***Infrastructure as a Service - IaaS.***

  Il consumatore ha facoltàdi acquisire elaborazione, memoria, rete e altre risorse fondamentali di calcolo, inclusi sistemi operativi e applicazioni. Anche in questo caso, il consumatore non gestisce ne controlla l'infrastruttura cloud sottostante, ma controlla sistemi operativi, memoria, applicazioni ed eventualmente, in modo limitato, alcuni componenti di rete (esempio firewalls).

È stato fatto riferimento, genericamente, ad un consumatore e fornitore di servizi cloud; in realtà è possibile identificare un insieme di attori che svolgono specifiche attività e funzioni nel processo di sviluppo dell'architettura del cloud. Si tratta del Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Auditor e Cloud Carrier.

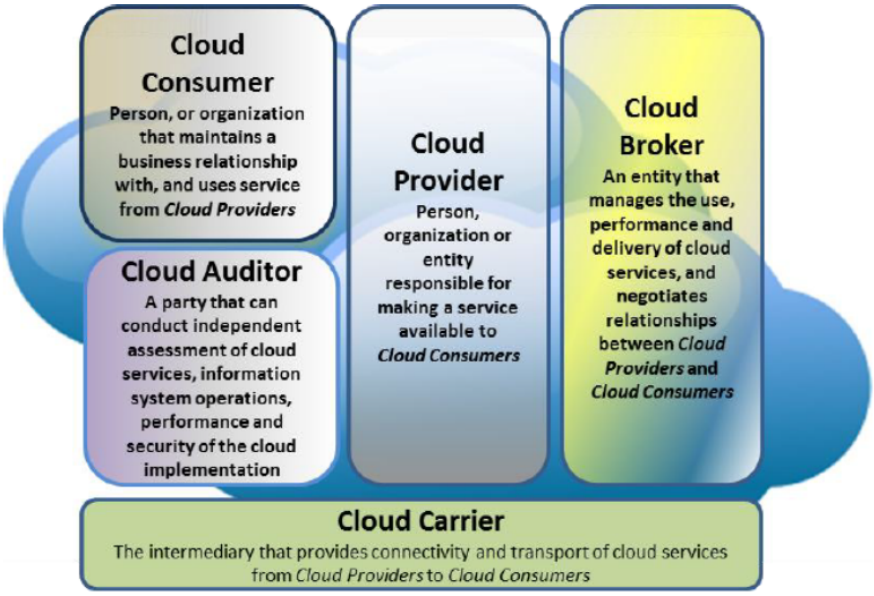

Figura 2. Attori del Cloud

Il ***cloud consumer*** è una persona/organizzazione che instaura una relazione di business con un cloud provider, per acquisire e usufruire dei suoi servizi. Tra le sue attività rientrano:

- l'analisi dei servizi di un determinato cloud provider ,
- la richiesta di appropriati servizi,
- impostazione del contratto dei servizi col cloud provider,
- utilizzo dei suoi servizi.

A seconda dei servizi richiesti, le attività e gli scenari possono essere differenti tra i vari consumer, in relazione al modello di servizio.
Ad esempio, nel modello SaaS, le applicazioni sono distribuite come servizi di hosting e sono accessibili mediante una rete che collega cloud consumer e cloud provider. In tale modello, i cloud consumer possono essere organizzazioni che forniscono l'accesso alle applicazioni ai loro membri che possono essere sia utenti finali che usano in modo diretto l'applicazione, sia amministratori che devono configurare le applicazioni, utilizzate dagli utenti finali.
Nel modello PaaS, invece, i cloud consumer impiegano strumenti e risorse messe a disposizione dal cloud provider per sviluppare, testare e gestire applicazioni in hosting su cloud. In questo caso, i cloud consumers

possono essere sia sviluppatori di applicazioni, sia amministratori che configurano e monitorano le prestazioni dell'applicazione su una piattaforma.
Nel modello IaaS, ai cloud consumer viene fornita la possibilità di accedere a varie risorse di elaborazione (come computer virtuali, storage accessibili mediante la rete, componenti per l'infrastruttura di rete), tramite le quali i cloud consumer possono eseguire e distribuire software. I cloud consumer possono essere sviluppatori, amministratori e responsabili IT interessati a creare, installare, gestire e monitorare servizi per operazioni inerenti infrastruttura IT.

Il ***cloud provider*** è una persona/organizzazione che crea e fornisce servizi per i cloud consumer. Nello specifico, si occupa di:

- creazione di servizi, piattaforme, infrastrutture richieste;
- gestione dell'infrastruttura necessaria per fornire servizi;
- distribuzione di servizi concordati;
- responsabile della sicurezza e della privacy dei servizi.

Anche in questo caso, a seconda dei modelli di servizio, il cloud provider ha ruoli differenti. Nel modello SaaS, il cloud provider impiega, configura, mantiene e supporta le applicazioni software su una determinata infrastruttura cloud; nel modello PaaS, gestisce l'infrastruttura cloud, fornisce strumenti e risorse affinché i cloud consumer possano sviluppare, testare e amministrare applicazioni sulla piattaforma; nel modello IaaS, gestisce e fornisce l'elaborazione fisica, lo storage, il networking, l'ambiente di hosting e l'infrastruttura cloud per i cloud consumer IaaS.

Service Models	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud system.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

Fig. 3 Consumer e Provider

Il ***cloud auditor*** è in grado di condurre una valutazione indipendente dei servizi cloud, delle operazioni del sistema informativo, delle prestazioni e della sicurezza da implementare nel cloud computing. Esso valuta i

servizi offerti da un cloud provider in termini di controllo della sicurezza, impatto sulla privacy, prestazioni e conformità dei parametri del contratto di servizio. I controlli di sicurezza riguardano la gestione, le operazioni e tecniche di salvaguardia o l'impiego di contromisure all'interno di un sistema informativo aziendale per proteggere la riservatezza, l'integrità e la disponibilità di un sistema. In merito ai controlli di sicurezza, un cloud auditor può effettuare una valutazione del controllo di sicurezza del sistema informativo per determinare in che misura i controlli sono implementati correttamente, se opera come previsto e producendo il risultato desiderato, in relazione ai requisiti di sicurezza per il sistema.

Il ***cloud broker*** è un intermediario tra il cloud consumer e il cloud provider.
Si occupa di guidare nella complessa scelta dei servizi cloud offerti e può, inoltre, creare dei servizi aggiuntivi. In generale, il cloud broker fornisce servizi suddivisi in tre categorie:

- Intermediazione - Un cloud broker migliora un determinato servizio perfezionando alcune funzionalità specifiche e fornendo servizi aggiuntivi ai cloud consumer. Il miglioramento può essere la gestione dell'accesso ai servizi cloud, gestione delle identità, reporting delle prestazioni, sicurezza avanzata, ecc.
- Aggregazione - Un cloud broker combina e integra servizi multipli in uno o più nuovi servizi, assicurando la sicurezza dei dati nel passaggio dal cloud consumer ai cloud provider multipli.
- Arbitraggio – similmente al servizio di arbitraggio, un broker ha la flessibilità di scegliere fra vari servizi messi a disposizione dei cloud provider.

Un cloud broker può fornire sia servizi di supporto alle imprese e alle relazioni, sia servizi di supporto tecnico.

Il ***cloud carrier*** agisce come un intermediario che fornisce la connettività e trasporto ai servizi cloud tra cloud consumer e cloud provider.

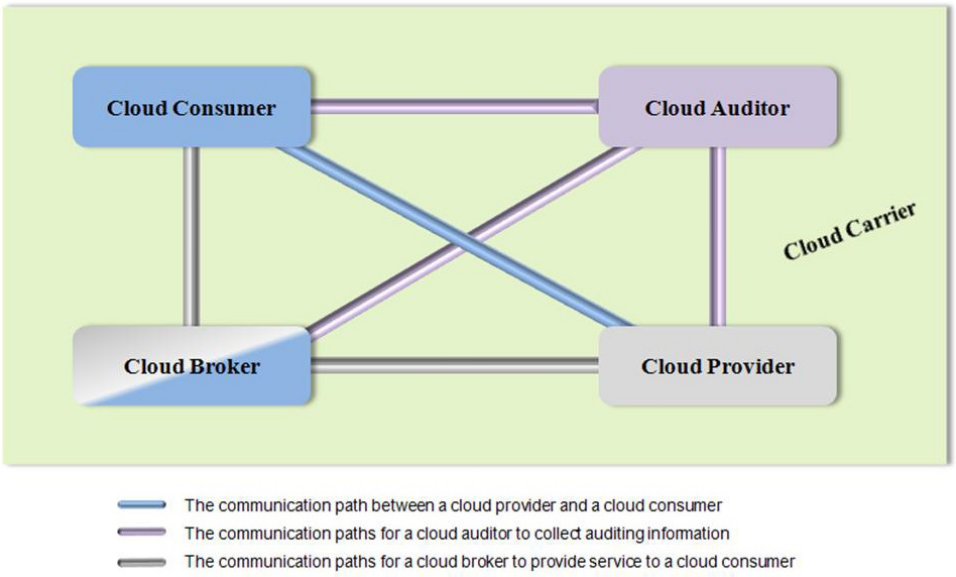

Fig.4 Network dei vari attori

Il NIST ha, inoltre, definito quattro modelli di distribuzione:

- ***Private Cloud***

  L'infrastruttura cloud è fornita per uso esclusivo di una singola organizzazione, comprendente molteplici consumatori (ad esempio filiali). Può essere posseduta, diretta e gestita dall'organizzazione stessa, da una società terza o da una combinazione delle due, e può esistere dentro o fuori le proprie sedi.

- ***Community Cloud.***

  L'infrastruttura cloud è fornita per uso esclusivo di una comunità di consumatori di organizzazioni con interessi comuni (ad esempio missione, requisiti di sicurezza, vincoli di condotta e di conformità). Può essere posseduta, diretta e gestita da una o più delle organizzazioni della comunità, da una società terza o una combinazione delle due e può esistere dentro o fuori le proprie sedi.

- ***Public Cloud.***

  L'infrastruttura cloud è fornita per un uso aperto a qualsiasi consumatore. Può essere posseduta, gestita da un'azienda, da un'organizzazione accademica o governativa oppure da una combinazione delle precedenti. Esiste dentro le sedi del fornitore cloud.

- ***Hybrid Cloud.***

  L'infrastruttura è una composizione di due o più infrastrutture cloud (privata, comunitaria o pubblica) che rimangono entità distinte, ma unite attraverso tecnologie standard o proprietarie, che abilitano la portabilità di dati e applicazioni (ad esempio per bilanciare il carico di lavoro tra cloud). Gli attori del cloud sono persone o organizzazioni che partecipano e/o eseguono compiti nel cloud e hanno un ruolo chiave nel cloud computing. Il NIST ha definito un'architettura di riferimento, uno strumento di alto livello che risulta importante per la definizione dei requisiti, della struttura e delle operazioni del cloud.

Diversi sono stati gli sviluppi tecnologici che hanno permesso la realizzazione di queste strutture cloud.
Lo sviluppo del cloud dunque è dovuto essenzialmente allo sviluppo della virtualizzazione hardware. Quest'ultima consente la condivisione dello stesso processore, a tanti sistemi operativi. Affinché possa essere sfruttata la virtualizzazione hardware, le CPU, i BIOS i sistemi operativi ed il software di virtualizzazione la devono supportare. Nelle architetture X86, Intel supporta la virtualizzazione hardware via VT-X extension, mentre AMD con la V extension. Anche le architetture ARM la forniscono attraverso la Large Physical Extension (LPAE).

Spesso vengono abusati o usati in maniera impropria alcuni concetti chiave della virtualizzazione, per cui è utile fare chiarezza su tali concetti:

- ***Hypervisor*** – Software, firmware, o hardware che crea ed avvia la macchina virtuale.
- ***Host OS / Machine*** – Sistema operativo o server su cui è installato l'Hypervisor
- ***Guest OS / Machine*** – La macchina virtuale che gira nell' hypervisor

Esistono diversi tipi di Hypervisor:

- Tipo 1: Nativo, o bare metal, hypervisor che vengono installati direttamente sull'hardware hostHyper-V (Microsoft), XenServer (Citrix), Vmware ESX/ESXi
- Tipo 2: Hosted, hypervisor che funzionano all'interno di sistemi operativi convenzionali. – VirtualBox (Oracle), VMWare Fusion, QEMU, Virtual PC, Parallels.

Non tutti gli hypervisor appartengono alle categorie Tipo 1 or Tipo 2. KVM, ad esempio, può essere visto sia come bare metal perché gira come modulo kernel, direttamente sull'hardware, e sia come tipo 2 in quanto esiste in linux come modulo kernel.

Precedentemente abbiamo già accennato alla macchina virtuale senza definirla;ebbene l'hypervisor fornisce accesso alle risorse virtualizzate quali CPUs, RAM, storage (dischi immagine), networking, BIOS, video, audio etc.., che insieme costituiscono la macchina virtuale in cui i sistemi operativi guest opereranno.
Alcuni Hypervisors forniscono dei tool che consentono l'interazione tra guest ed host.
Per esempio, Virtula Box ha delle guest additions che consentono la condivisione delle cartelle tra guest e host, taglia, incolla ed altre funzioni. Queste funzionalità, però, non sono disponibili per tutti I sistemi operativi intelligenti e altri dispositivi. I suoi utilizzi annoverano la raccolta di dati operativi da sensori remoti su piattaforme petrolifere, la raccolta di dati meteorologici e il controllo di termostati intelligenti.
Una macchina virtuale ben poco sarebbe se non ci fossero anche i cosiddetti dischi immagine. Il discoimmagine include,fondamentalmente, i contenuti necessari alla virtual machine. Ci sono diversi formati per queste immagini:

• raw formato binario in chiaro,
• qcow2 formato QEMU cioè quello fornito dal virtualizzatore hardware QEMU https://www.qemu.org/, usato da KVM,
• vmdk Virtual machine Disk (VMWARE)
• vdi Virtual Disk Image (Virtual Box)
• vhd Virtual Hard Disk (Microsoft).

Per questi ambienti virtualizzati, è di particolare importanza il formato Open Virtualization Format (OVF), Si tratta di unaspecifica(https://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0. pdf), definita dall'organizzazione Data Management Task Force (DMTF), che ha lo scopo di consentire l'interscambio di virtual machine tra diversi hypervisor, indipendentemente dall'architettura del processore sottostante. Questo formato contiene, oltre all'immagine disco, anche dei meta dati riguardanti la virtual machine. Il tutto viene distribuito adottando un file con estensione OVA che è un tar delle informazioni OVF. Molto spesso si ricorre a delle immagini disco già "preconfezionate" (prebuilt), che consentono di ridurre ulteriormente i tempi di messa in campo delle VM, evitando tutta la fase di installazione del sistema operativo. Quando si usano queste immagini , è importante curarsi della sorgenti da cui si prelevano, per motivi legati evidentemente alla sicurezza. E' consigliato, qualora il prodotto debba essere messo in produzione, procedere all'installazione del proprio sistema da scratch. Per esempio, Oracle produce diversi dischi immagine, incluso Solaris 10 e Solaris 11 x86 ed anche Oracle Linux.
Chiaramente senza licenza queste immagini non si possono usare in produzione.
Oracle con Virtual Box(https://www.virtualbox.org/) offre altre immagini di altri sistemi operativi molto diffusi, quali Ubuntu, Debian, Centos e Fedora.

Da applicazione locale a CLOUD

Una qualunque applicazione può essere "virtualizzata" usando Hypervisor SW su di un server locale.Un Hyperivisor può supportare, contemporaneamente, diversi sistemi operativi e di conseguenza diverse tipologie di applicazioni.

L'uso della virtualizzazione consente dunque, dato un server, di sfruttare intensivamente l'hardware disponibile; inoltre, consente l'handling in maniera efficiente di applicazioni di diversi tipi, mantenendo il costo degli equipment molto basso.
Se la necessità è quella di avere diverse applicazioni distribuite su server multipli e distribuite in diversi data center la parola "chiave" è Cloud.
Esposti i concettibase per lo sviluppo del cloud, ovvero quello di macchina virtuale e dischi immagine, passiamo a presentare brevemente uno dei software, open source, maggiormente utilizzato per la realizzazione di CLOUD pubblico e Privato:***Open Stack*** (https://www.openstack.org/).

È sviluppato in Python e le interfacce tra i vari componenti che lo costituiscono sono di tipo RESTFul.
I componenti software fondamentali della piattaforma sono essenzialmente 6:
NOVA il controllore delle risorse computazionali,
SWIFT sistema di storage di oggetti distribuiti,
GLANCE Servizio per la gestione delle immagini dei dischi virtuali,
HORIZON Dashboard (interfaccia grafica),
KEYSTONE Dedicato all'autenticazione degli utenti NEUTRON dedicato al network management,
CINDER sistema per la gestione di blocchi di storage persistenti.

La piattaforma Open Stack ha dei rilasci semestrali, ed attualmente l'ultima release è Rocky.
Allo sviluppo di questa piattaforma open source contribuiscono colossi del software e delle telecomunicazioni , denotando il chiaro interesse che c'è nei confronti della stessa.

Esistono dei rischi per la sicurezza?

La protezione dei sistemi informativi, la garanzia della riservatezza, dell'integrità e della disponibilità delle informazioni e del trattamento, memorizzazione e trasmissione delle stesse sono preoccupazioni prioritarie e presentano un elevato rischio di essere compromesse nel cloud computing. Come abbiamo già visto, il cloud computing supporta tre modelli di servizio, quattro modelli di distribuzione e cinque caratteristiche essenziali che comportano una certa complessità nell'architettura. È evidente come con l'aggiunta della multi-tenancy, siaaumentata ancor di più la necessità di dover proteggere i dati.

I rischi per la sicurezza, sono legati alla compromissione della riservatezza e dell'integrità dei dati in transito da o verso un cloud provider,alle vulnerabilità esistenti, alla limitata abilità nel crittografare dati in un ambiente multi-tenancy e all'intercettazione dei dati in transito (attacchi man-in-the-middle).

Secondo il NIST, a tutela della sicurezza dei dati, è fondamentale:

- garantire la protezione dei dati da accessi non autorizzati;
- impedire l'accesso alle risorse dell'infrastruttura cloud, ai soggetti non autorizzati;
- includere sistemi per il controllo degli accessi.

Responsabilità e modelli di sicurezza

Partendo dall'assunto che il cloud computing è una tecnologia basata sulla condivisione di informazioni, dove differenti organizzazioni sono responsabili dell'implementazione e gestione delle varie parti, è chiaro come ciò implichi una distribuzione delle responsabilità di sicurezza tra le varie organizzazioni coinvolte. Si parla in questo caso, difatti, di modello a responsabilità condivisa.

Per i differenti modelli di servizio, la responsabilità della sicurezza corrisponde al grado di controllo di ciascun attore:

- *SaaS*, il cloud provider è responsabile di quasi tutta la sicurezza, il cloud consumer può solo accedere e gestire l'uso dell'applicazioni senza alterare il funzionamento.
- *PaaS*, il cloud provider è il responsabile della sicurezza dell'infrastruttura, mentre il cloud consumer è responsabile di tutto ciò che implementa nella stessa, inclusa la configurazione delle funzionalità di sicurezza.
- *IaaS*, il cloud provider è responsabile della sicurezza di base mentre il cloud consumer è responsabile di qualsiasi cosa che implementa nell'infrastruttura; in questo caso il cloud consumer ha maggiore responsabilità.

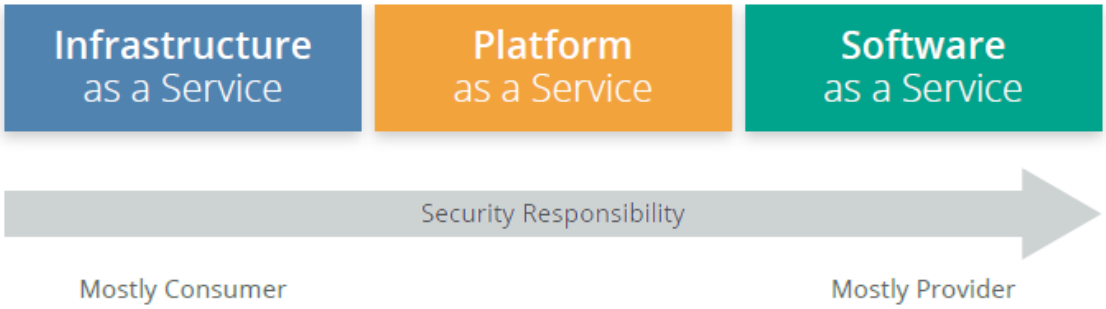

Figura 5. Grado di responsabilità della sicurezza

Essenzialmente spetta ai cloud provider documentare, in maniera chiara, i controlli di sicurezza interni e la funzionalità di sicurezza in modo da supportare i cloud consumer nelle decisioni. Al tempo stesso, i cloud consumer dovrebbero definire una matrice di responsabilità per documentare chi implementa i controlli e come.

Per garantire, quindi, la sicurezza del cloud, è possibile ricorrere a dei modelli che consentono di limitare l'esposizione ai possibili rischi:

- Modelli o framework concettuali - includono descrizioni usate per spiegare i concetti e i principi di sicurezza del cloud,
- Modelli o framework di controllo - categorizzano e descrivono, in modo specifico, i controlli di sicurezza nel cloud o categorie di controlli.
- Architetture di riferimento - template per implementare la sicurezza del cloud, tipicamente generalizzata.
- Pattern di progettazione - soluzioni riusabili per particolari problemi.

Inoltre, è possibile adoperare un processo per la gestione della sicurezza in ambito cloud:

  - identificare i requisiti necessari di sicurezza e i controlli già esistenti;
  - selezionare il provider, il modello di servizio e di distribuzione;
  - definire l'architettura;
  - stimare i controlli di sicurezza;
  - identificare le lacune di controllo;
  - progettare e implementare controlli per colmare le lacune;
  - gestire le modifiche nel tempo.

Tra queste, le azioni basilari sono l'identificazione dei requisiti, la progettazione dell'architettura e poi l'individuazione delle lacune basandosi sulle capacità dell'infrastruttura cloud sottostante.
Tutto ciò necessita, ovviamente,la definizione del provider e dell'architettura, prima di iniziare a tradurre i requisiti di sicurezza nei controlli.

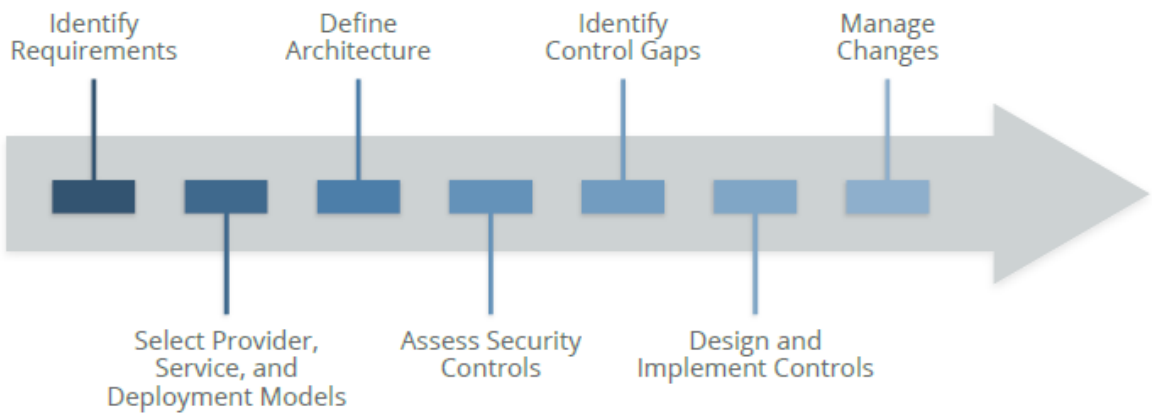

Figura 6. Modello semplificato per la gestione della sicurezza

Focus sull'aree critiche

Il CSA – Cloud Security Alliance ha individuato 13 domini, aree di interesse per il cloud computing che sono state messe insieme per affrontare al meglio i punti critici in relazione alla strategia di sicurezza da apportare;strategia che può essere applicata a qualsiasi combinazione modello di servizio modello di distribuzione. Le aree di interesse, sono state divise due categorie: governance e operating.

La categoria governance è più ampia e affronta strategie e politiche da attuare all'interno del cloud;l'operating si concentra, invece, sulla strategia di sicurezza e della sua implementazione dall'interno del cloud.

I domini che fanno parte della categoria governance sono:

- **Governance and Enterprise Risk Management:** La capacità di un'organizzazione di governare e misurare i rischi aziendali introdotti dal cloud computing.
- **Legal Issues:**Contracts and Electronic Discovery Potenziali problemi legali quando si utilizza il cloud computing.
- **Compliance and Audit Management:** Mantenimento e dimostrazione della conformità quando si utilizza il cloud computing.
- **Information Governance:** controllo dei dati che vengono inseriti nel cloud.
- **Management Plan and Business Continuity:** Protezione del piano di gestione e delle interfacce amministrative utilizzate durante l'accesso al cloud, comprese le console Web e le Application Programming Interface - API per garantire la continuità aziendale per le distribuzioni cloud.

I domini che fanno parte della categoria operating sono:

- ***Infrastructure Security***: il nucleo della sicurezza dell'infrastruttura del cloud, tra cui networking, sicurezza del workload e considerazioni sul cloud ibrido. Questo dominio include anche i fondamenti della sicurezza per i cloud privati.
- ***Virtualization and Containers***: Sicurezza per hypervisor, container e Software Defined Networking – SDN .
- ***IncidentResponse, Notification and Remediation***: giusta e adeguata rilevazione, risposta, notifica e rimedio agli incidenti.
- ***Application Security***: protezione del software applicativo in esecuzione o in fase di sviluppo nel cloud. Ciò include elementi quali il trasferimento o la progettazione di un'applicazione da

eseguire nel cloud e, in caso affermativo, il tipo di piattaforma cloud più appropriata (SaaS, PaaS o IaaS).

- ***Data Security and Encryption***: implementazione della sicurezza e della crittografia dei dati e garanzia della gestione scalabile delle chiavi.
- ***Identity, Entitlement, and Access Management***: gestire le identità e sfruttare i servizi di directory per fornire il controllo degli accessi. L'attenzione si concentra sui problemi riscontrati durante l'estensione dell'identità di un'organizzazione nel cloud. Questa sezione fornisce informazioni dettagliate sulla valutazione della disponibilità di un'organizzazione a condurre Identity, Entitlement e Access Management (IdEA) basati su cloud.
- ***Security as a Service***: fornire la garanzia della sicurezza facilitata da parte di terzi, la gestione degli incidenti, l'attestato di conformità, l'identità e la supervisione dell'accesso.
- ***Related Technologies***: tecnologie affermate ed emergenti, in relazione col cloud computing, compresi Big Data , Internet of Things e mobile computing.
    - *API:* indica ogni insieme di procedure disponibili al programmatore, di solito raggruppate a formare un set di strumenti specifici per adempire un determinato compito all'interno di un certo programma. Spesso con API intendiamo librerie software disponibili per un determinato linguaggio di programmazione.
    - *SDN* è un paradigma che promette di trasformare i network tradizionali in piattaforme flessibili e intelligenti, per rispondere in tempo reale, alle esigenze di larghezza di banda e alla natura dinamica delle moderne applicazioni.
    - *Big Data* è un termine adoperato per descrivere l'insieme delle tecnologie e delle metodologie di analisi di dati massivi. Il termine indica la capacità di estrapolare, analizzare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non strutturati, per scoprire i legami tra fenomeni diversi e prevedere quelli futuri.
    - *Internet of Things* sta a indicare il cospicuo e crescente insieme di dispositivi digitali (ormai miliardi) che operano in reti su scala potenzialmente mondiale. A differenza dell'Internet normale (delle persone), l'IoT comprende solo sensori.