



## A. Cloud computing

---

Il cloud computing è la disponibilità su richiesta delle risorse del sistema informatico, in particolare l'archiviazione dei dati e la potenza di elaborazione, senza una gestione attiva diretta da parte dell'utente. Il termine viene generalmente utilizzato per descrivere i data center disponibili per molti utenti su Internet. I cloud di grandi dimensioni, oggi predominanti, hanno spesso funzioni distribuite su più posizioni dai server centrali. Se la connessione con l'utente è relativamente stretta, può essere designato un server perimetrale.

I cloud possono essere limitati a una singola organizzazione (cloud aziendali) o essere disponibili per molte organizzazioni (cloud pubblico).

Il cloud computing si basa sulla condivisione delle risorse per ottenere coerenza ed economie di scala.

I sostenitori del cloud pubblico e ibrido osservano che il cloud computing consente alle aziende di evitare o minimizzare i costi iniziali dell'infrastruttura IT. I sostenitori affermano inoltre che il cloud computing consente alle aziende di mettere in funzione le loro applicazioni più velocemente, con una migliore gestibilità e meno manutenzione, e che consente ai team IT di adattare più rapidamente le risorse per soddisfare la domanda fluttuante e imprevedibile. I fornitori di servizi cloud in genere utilizzano un modello "pay-as-you-go", che può comportare spese operative impreviste se gli amministratori non hanno familiarità con i modelli di determinazione del prezzo del cloud.

La disponibilità di reti ad alta capacità, computer e dispositivi di archiviazione a basso costo, nonché l'adozione diffusa di virtualizzazione hardware, architettura orientata ai servizi e calcolo autonomo e di utilità ha portato alla crescita del cloud computing. Entro il 2019, Linux era il sistema operativo più utilizzato, incluso nelle offerte di Microsoft ed è quindi descritto come dominante. Il Cloud Service Provider (CSP) controllerà, manterrà e raccoglierà i dati relativi ai firewall, all'identificazione delle intrusioni o / e ai framework di azioni contrarie e flusso di informazioni all'interno della rete.

### A.1. Qual è il cloud

---

L'obiettivo del cloud computing è consentire agli utenti di beneficiare di tutte queste tecnologie, senza la necessità di una conoscenza approfondita o esperienza con ognuna di esse. Il cloud mira a ridurre i costi e aiuta gli utenti a concentrarsi sul proprio core business invece di essere ostacolati da ostacoli IT. La principale tecnologia abilitante per il cloud computing è la virtualizzazione. Il software di virtualizzazione separa un dispositivo di elaborazione fisica in uno o più dispositivi "virtuali", ognuno dei quali può essere facilmente utilizzato e gestito per eseguire attività di elaborazione. Con la virtualizzazione a livello di sistema operativo essenzialmente creando un sistema scalabile di più dispositivi di elaborazione indipendenti, le risorse di elaborazione inattive possono essere allocate e utilizzate in modo più efficiente. La virtualizzazione fornisce l'agilità necessaria per accelerare le operazioni IT e riduce i costi aumentando l'utilizzo dell'infrastruttura. Il calcolo autonomo automatizza il processo attraverso il quale l'utente può fornire risorse su richiesta. Riducendo al minimo il coinvolgimento degli utenti, l'automazione accelera il processo, riduce i costi di manodopera e riduce la possibilità di errori umani.

Il cloud computing utilizza i concetti dell'utility computing per fornire metriche per i servizi utilizzati. Il cloud computing tenta di affrontare i problemi di qualità del servizio e di affidabilità di altri modelli di grid computing.

Il cloud computing condivide le caratteristiche con:



- Modello client-server: il calcolo client-server si riferisce ampiamente a qualsiasi applicazione distribuita che distingue tra provider di servizi (server) e richiedenti di servizi (client).
- Computer bureau: un ufficio servizi che fornisce servizi informatici, in particolare dagli anni '60 agli anni '80.
- Grid computing: una forma di calcolo distribuito e parallelo, in base al quale un "computer super e virtuale" è composto da un gruppo di computer collegati in rete, liberamente accoppiati, che agiscono in concerto per svolgere compiti molto grandi.
- Nebbia informatica: paradigma di elaborazione distribuita che fornisce servizi di dati, elaborazione, archiviazione e applicazioni più vicini ai dispositivi client o near-user edge, come i router di rete. Inoltre, il fog computing gestisce i dati a livello di rete, su dispositivi intelligenti e sul lato client dell'utente finale (ad esempio dispositivi mobili), anziché inviare dati a una posizione remota per l'elaborazione.
- Computer mainframe: computer potenti utilizzati principalmente da grandi organizzazioni per applicazioni critiche, in genere l'elaborazione di dati in blocco come: censimento; statistiche dell'industria e dei consumatori; polizia e servizi segreti; pianificazione delle risorse aziendali; e l'elaborazione delle transazioni finanziarie.
- Utility computing: il "pacchetto di risorse informatiche, come il calcolo e l'archiviazione, come un servizio misurato simile a un'utilità pubblica tradizionale, come l'elettricità".
- Peer-to-peer: un'architettura distribuita senza la necessità di un coordinamento centrale. I partecipanti sono sia fornitori che consumatori di risorse (contrariamente al tradizionale modello client-server).
- Green computing
- Cloud sandbox: un ambiente informatico attivo e isolato in cui un programma, un codice o un file può essere eseguito senza influire sull'applicazione in cui viene eseguito.

## A.2. Caratteristiche

Il cloud computing presenta le seguenti caratteristiche chiave:

- L'agilità per le organizzazioni può essere migliorata, poiché il cloud computing può aumentare la flessibilità degli utenti con il provisioning, l'aggiunta o l'espansione delle risorse dell'infrastruttura tecnologica.
- Le riduzioni dei costi sono richieste dai fornitori di servizi cloud. Un modello di distribuzione su cloud pubblico converte le spese in conto capitale (ad esempio, l'acquisto di server) in spese operative. Ciò presumibilmente riduce gli ostacoli all'ingresso, poiché l'infrastruttura è in genere fornita da una terza parte e non deve essere acquistata per attività di elaborazione intensive una tantum o rare. Il prezzo su base informatica è "a grana fine", con opzioni di fatturazione basate sull'utilizzo. Inoltre, sono necessarie meno competenze IT interne per l'implementazione di progetti che utilizzano il cloud computing. Il repository all'avanguardia del progetto e-FISCAL<sup>[47]</sup> contiene numerosi articoli che esaminano più dettagliatamente gli aspetti dei costi, molti dei quali concludono che i risparmi sui costi dipendono dal tipo di attività sostenute e dal tipo di infrastruttura disponibile internamente.
- Indipendenza dal dispositivo e dalla posizione consente agli utenti di accedere ai sistemi utilizzando un browser Web indipendentemente dalla loro posizione o dal dispositivo che utilizzano (ad es. PC, telefono cellulare). Poiché l'infrastruttura è off-site (in genere fornita da una terza parte) e accessibile tramite Internet, gli utenti possono connettersi ad essa da qualsiasi luogo.
- La manutenzione delle applicazioni di cloud computing è più semplice, poiché non devono essere installate sul computer di ciascun utente e sono accessibili da luoghi diversi (ad esempio, luoghi di lavoro diversi, durante i viaggi, ecc.).
- La multi-tenancy consente la condivisione di risorse e costi attraverso un ampio pool di utenti consentendo così:
  - centralizzazione delle infrastrutture in luoghi con costi inferiori (come immobili, elettricità, ecc.)
  - aumenta la capacità di carico massimo (gli utenti non devono progettare e pagare le risorse e le attrezzature per raggiungere i livelli di carico più elevati possibili)
  - utilizzo e miglioramenti dell'efficienza per i sistemi che sono spesso utilizzati solo dal 10-20%.



- Le prestazioni sono monitorate da esperti IT del fornitore di servizi e architetture coerenti e liberamente accoppiate sono costruite utilizzando i servizi Web come interfaccia di sistema.
- La produttività può essere aumentata quando più utenti possono lavorare sugli stessi dati contemporaneamente, invece di attendere che vengano salvati e inviati via e-mail. È possibile che si risparmi tempo poiché non è necessario reinserire le informazioni quando i campi sono abbinati, né gli utenti devono installare aggiornamenti del software applicativo sul proprio computer.
- L'affidabilità migliora con l'uso di più siti ridondanti, il che rende il cloud computing ben progettato adatto alla continuità aziendale e al ripristino di emergenza.
- Scalabilità ed elasticità tramite provisioning dinamico ("on demand") di risorse su base self-service a grana fine quasi in tempo reale (Nota, il tempo di avvio della VM varia in base al tipo di VM, alla posizione, Sistemi operativi e fornitori di cloud), senza che gli utenti debbano progettare i carichi di picco. Ciò offre la possibilità di aumentare le dimensioni quando aumenta o diminuisce l'utilizzo delle risorse se non vengono utilizzate risorse. Gli approcci emergenti per la gestione dell'elasticità includono l'uso di tecniche di apprendimento automatico per proporre modelli di elasticità efficienti.<sup>[60]</sup>
- La sicurezza può migliorare grazie alla centralizzazione dei dati, all'aumento delle risorse incentrate sulla sicurezza, ecc., Ma possono persistere dubbi sulla perdita di controllo su alcuni dati sensibili e sulla mancanza di sicurezza per i kernel archiviati. La sicurezza è spesso buona o migliore di altri sistemi tradizionali, in parte perché i fornitori di servizi sono in grado di dedicare risorse per risolvere problemi di sicurezza che molti clienti non possono permettersi di affrontare o ai quali mancano le competenze tecniche per affrontare. Tuttavia, la complessità della sicurezza aumenta notevolmente quando i dati vengono distribuiti su un'area più ampia o su un numero maggiore di dispositivi, nonché in sistemi multi-tenant condivisi da utenti indipendenti. Inoltre, l'accesso degli utenti ai registri di controllo della sicurezza può essere difficile o impossibile. Le installazioni di cloud privato sono in parte motivate dal desiderio degli utenti di mantenere il controllo sull'infrastruttura ed evitare di perdere il controllo della sicurezza delle informazioni.

La definizione di cloud computing del National Institute of Standards and Technology identifica "cinque caratteristiche essenziali":

**Self service su richiesta.** Un consumatore può fornire unilateralmente funzionalità di elaborazione, come il tempo del server e l'archiviazione di rete, secondo necessità automaticamente senza richiedere l'interazione umana con ciascun fornitore di servizi.

**Ampio accesso alla rete.** Le funzionalità sono disponibili sulla rete e sono accessibili attraverso meccanismi standard che promuovono l'uso da parte di piattaforme client eterogenee sottili o spesse (ad esempio telefoni cellulari, tablet, laptop e workstation).

**Pooling di risorse.** Le risorse informatiche del provider sono raggruppate per servire più consumatori utilizzando un modello multi-tenant, con diverse risorse fisiche e virtuali assegnate e riassegnate dinamicamente in base alla domanda dei consumatori.

**Rapida elasticità.** Le capacità possono essere fornite e liberate elasticamente, in alcuni casi automaticamente, per ridimensionarsi rapidamente verso l'esterno e verso l'interno in proporzione alla domanda. Al consumatore, le funzionalità disponibili per il provisioning spesso appaiono illimitate e possono essere appropriate in qualsiasi quantità in qualsiasi momento.

**Servizio misurato.** I sistemi cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse sfruttando una capacità di misurazione a un certo livello di astrazione adeguata al tipo di servizio (ad es. Archiviazione, elaborazione, larghezza di banda e account utente attivi). L'utilizzo delle risorse può essere monitorato, controllato e segnalato, garantendo trasparenza sia per il fornitore che per il consumatore del servizio utilizzato.

- National Institute of Standards and Technology



## A.3. Modelli di servizio

Sebbene l'architettura orientata ai servizi sostenga "Tutto come un servizio" (con gli acronimi EaaS o XaaS, [63] o semplicemente aas), i fornitori di cloud computing offrono i loro "servizi" in base a diversi modelli, di cui i tre modelli standard per NIST sono Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). [62] Questi modelli offrono astrazione crescente; sono quindi spesso rappresentati come livelli in uno stack: infrastruttura, piattaforma e software come servizio, ma questi non devono essere correlati. Ad esempio, si può fornire SaaS implementato su macchine fisiche (bare metal), senza utilizzare i livelli PaaS o IaaS sottostanti, e viceversa si può eseguire un programma su IaaS e accedervi direttamente, senza avvolgerlo come SaaS.

### A.1.1. Infrastruttura come servizio (IaaS)

*Articolo principale: Infrastruttura come servizio*

"Infrastruttura come servizio" (IaaS) si riferisce a servizi online che forniscono API di alto livello utilizzate per dereferenziare vari dettagli di basso livello dell'infrastruttura di rete sottostante come risorse di elaborazione fisica, posizione, partizionamento dei dati, ridimensionamento, sicurezza, backup ecc. Un hypervisor esegue le macchine virtuali come ospiti. I pool di hypervisor all'interno del sistema operativo cloud possono supportare un gran numero di macchine virtuali e la capacità di scalare i servizi su e giù in base alle diverse esigenze dei clienti. I contenitori Linux vengono eseguiti in partizioni isolate di un singolo kernel Linux in esecuzione direttamente sull'hardware fisico. I cgroup e gli spazi dei nomi di Linux sono le tecnologie del kernel Linux sottostanti utilizzate per isolare, proteggere e gestire i contenitori. La containerizzazione offre prestazioni più elevate rispetto alla virtualizzazione, poiché non esiste un sovraccarico di hypervisor. Inoltre, la capacità del contenitore si ridimensiona automaticamente in base al carico di elaborazione, il che elimina il problema del provisioning eccessivo e consente la fatturazione basata sull'utilizzo. I cloud IaaS spesso offrono risorse aggiuntive come una libreria di immagini del disco di una macchina virtuale, archiviazione a blocchi grezzi, archiviazione di file o oggetti, firewall, bilanciamento del carico, indirizzi IP, reti locali virtuali (VLAN) e bundle di software.

La definizione di cloud computing del NIST descrive IaaS come "in cui il consumatore è in grado di distribuire ed eseguire software arbitrario, che può includere sistemi operativi e applicazioni. Il consumatore non gestisce o controlla l'infrastruttura cloud sottostante ma ha il controllo sui sistemi operativi, sull'archiviazione, e applicazioni distribuite e possibilmente controllo limitato di componenti di rete selezionati (ad esempio, firewall host)."

I fornitori di cloud IaaS forniscono queste risorse su richiesta dai loro grandi pool di apparecchiature installate nei data center. Per la connettività su vasta area, i clienti possono utilizzare Internet o carrier cloud (reti private virtuali dedicate). Per distribuire le loro applicazioni, gli utenti cloud installano le immagini del sistema operativo e il loro software applicativo sull'infrastruttura cloud. In questo modello, l'utente cloud corregge e mantiene i sistemi operativi e il software applicativo. I fornitori di servizi cloud in genere fatturano i servizi IaaS su una base di calcolo di utilità: il costo riflette la quantità di risorse allocate e consumate.

### A.1.2. Platform as a service (PaaS)

La definizione di cloud computing del NIST definisce Platform as a Service come:

La capacità fornita al consumatore è quella di implementare nell'infrastruttura cloud applicazioni create o acquisite dal consumatore create utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal provider. Il consumatore non gestisce o controlla l'infrastruttura cloud sottostante, inclusi rete, server, sistemi operativi o archiviazione, ma ha il controllo sulle applicazioni distribuite e possibilmente le impostazioni di configurazione per l'ambiente di hosting delle applicazioni.

I fornitori di PaaS offrono agli sviluppatori di applicazioni un ambiente di sviluppo. Il provider in genere sviluppa toolkit e standard per lo sviluppo e canali per la distribuzione e il pagamento. Nei modelli PaaS, i fornitori di servizi cloud offrono una piattaforma di elaborazione, in genere comprendente sistema operativo, ambiente di esecuzione del linguaggio di programmazione,



database e server Web. Gli sviluppatori di applicazioni sviluppano ed eseguono il loro software su una piattaforma cloud anziché acquistare e gestire direttamente i livelli hardware e software sottostanti. Con alcuni PaaS, il computer e le risorse di archiviazione sottostanti si ridimensionano automaticamente per soddisfare la domanda dell'applicazione in modo che l'utente del cloud non debba allocare risorse manualmente.

Alcuni provider di integrazione e gestione dei dati utilizzano anche applicazioni specializzate di PaaS come modelli di consegna dei dati. Gli esempi includono iPaaS (Integration Platform as a Service) e dPaaS (Data Platform as a Service). iPaaS consente ai clienti di sviluppare, eseguire e governare i flussi di integrazione. Secondo il modello di integrazione iPaaS, i clienti guidano lo sviluppo e la distribuzione di integrazioni senza installare o gestire alcun hardware o middleware. dPaaS offre prodotti di integrazione e gestione dei dati come servizio completamente gestito. In base al modello dPaaS, il fornitore PaaS, non il cliente, gestisce lo sviluppo e l'esecuzione di programmi creando applicazioni di dati per il cliente. Gli utenti di dPaaS accedono ai dati tramite strumenti di visualizzazione dei dati. I consumatori di Platform as a Service (PaaS) non gestiscono o controllano l'infrastruttura cloud sottostante, inclusi rete, server, sistemi operativi o archiviazione, ma hanno il controllo delle applicazioni distribuite e possibilmente delle impostazioni di configurazione per l'ambiente di hosting delle applicazioni.

### **A.1.3. Software as a service (SaaS)**

La definizione di cloud computing del NIST definisce Software as a Service come:

La capacità fornita al consumatore è di utilizzare le applicazioni del provider in esecuzione su un'infrastruttura cloud. Le applicazioni sono accessibili da vari dispositivi client tramite un'interfaccia thin client, ad esempio un browser Web (ad esempio, e-mail basata sul Web) o un'interfaccia di programma. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante, inclusi rete, server, sistemi operativi, spazio di archiviazione o persino singole funzionalità dell'applicazione, con la possibile eccezione di impostazioni di configurazione dell'applicazione specifiche dell'utente limitate.

Nel modello software as a service (SaaS), gli utenti ottengono l'accesso al software applicativo e ai database. I provider cloud gestiscono l'infrastruttura e le piattaforme che eseguono le applicazioni. A volte SaaS viene definito "software su richiesta" e di solito ha un prezzo pay-per-use o utilizzando un canone di abbonamento. Nel modello SaaS, i provider cloud installano e gestiscono software applicativo nel cloud e gli utenti cloud accedono al software dai client cloud. Gli utenti cloud non gestiscono l'infrastruttura e la piattaforma cloud su cui è in esecuzione l'applicazione. Ciò elimina la necessità di installare ed eseguire l'applicazione sui propri computer dell'utente cloud, semplificando la manutenzione e il supporto. Le applicazioni cloud differiscono dalle altre applicazioni per la loro scalabilità, cosa che può essere ottenuta clonando attività su più macchine virtuali in fase di esecuzione per soddisfare le mutevoli richieste di lavoro. I servizi di bilanciamento del carico distribuiscono il lavoro sull'insieme di macchine virtuali. Questo processo è trasparente per l'utente cloud, che vede un solo punto di accesso. Per soddisfare un gran numero di utenti cloud, le applicazioni cloud possono essere multi-tenant, il che significa che qualsiasi macchina può servire più di un'organizzazione cloud-utente.

Il modello di determinazione del prezzo per le applicazioni SaaS è in genere una tariffa forfettaria mensile o annuale per utente, pertanto i prezzi diventano scalabili e regolabili se gli utenti vengono aggiunti o rimossi in qualsiasi momento. Potrebbe anche essere gratuito. I sostenitori affermano che SaaS offre alle aziende il potenziale per ridurre i costi operativi IT esternalizzando la manutenzione e il supporto hardware e software al provider cloud. Ciò consente all'azienda di riallocare i costi delle operazioni IT lontano dalle spese hardware / software e dalle spese del personale, verso il raggiungimento di altri obiettivi. Inoltre, con le applicazioni ospitate centralmente, gli aggiornamenti possono essere rilasciati senza la necessità per gli utenti di installare nuovo software. Uno svantaggio di SaaS è rappresentato dalla memorizzazione dei dati degli utenti sul server del provider cloud. Di conseguenza, potrebbe esserci un accesso non autorizzato ai dati. Esempi di applicazioni offerte come SaaS sono giochi e software di produttività come Google Docs e Word Online. Le applicazioni SaaS possono essere integrate con l'archiviazione cloud o i servizi di file hosting, come nel caso di Google Docs integrato con Google Drive e Word Online integrato con Onedrive.



#### **A1.4.Backend mobile come servizio**

*Articolo principale: backend mobile come servizio*

Nel modello "backend" as a service (m) mobile, noto anche come backend as a service (BaaS), agli sviluppatori di app Web e app mobili viene fornito un modo per collegare le loro applicazioni allo storage cloud e ai servizi di cloud computing con la programmazione delle applicazioni interfacce (API) esposte alle loro applicazioni e kit di sviluppo software personalizzati (SDK). I servizi comprendono la gestione degli utenti, le notifiche push, l'integrazione con i servizi di social network e altro ancora. Questo è un modello relativamente recente nel cloud computing, con la maggior parte delle startup BaaS risalenti al 2011 o in seguito, ma le tendenze indicano che questi servizi stanno guadagnando una significativa tendenza mainstream con i consumatori aziendali.

#### **A.1.5. Elaborazione senza server**

Il serverless computing è un modello di esecuzione del codice di cloud computing in cui il provider cloud gestisce completamente l'avvio e l'arresto delle macchine virtuali in base alle necessità per soddisfare le richieste e le richieste vengono fatturate da una misura astratta delle risorse necessarie per soddisfare la richiesta, anziché per macchina virtuale, all'ora. Nonostante il nome, in realtà non implica l'esecuzione di codice senza server. L'elaborazione senza server è così denominata perché l'azienda o la persona proprietaria del sistema non deve acquistare, noleggiare o eseguire il provisioning di server o macchine virtuali per l'esecuzione del codice back-end.

#### **A.1.6. Funzione come servizio (FaaS)**

La funzione come servizio (FaaS) è una chiamata di procedura remota ospitata da un servizio che sfrutta l'elaborazione senza server per consentire l'implementazione di singole funzioni nel cloud eseguite in risposta a eventi. FaaS è incluso nel termine serverless computing a più ampio termine, ma i termini possono anche essere usati in modo intercambiabile.

### **A.4. Modelli di distribuzione**

#### **A.1.7. Cloud privato**

Il cloud privato è un'infrastruttura cloud gestita esclusivamente per una singola organizzazione, gestita internamente o da una terza parte, e ospitata internamente o esternamente. La realizzazione di un progetto di cloud privato richiede un impegno significativo per virtualizzare l'ambiente aziendale e richiede all'organizzazione di rivalutare le decisioni sulle risorse esistenti. Può migliorare il business, ma ogni fase del progetto solleva problemi di sicurezza che devono essere affrontati per prevenire gravi vulnerabilità. I data center self-run [84] sono generalmente ad alta intensità di capitale. Hanno un'impronta fisica significativa, che richiede allocazioni di spazio, hardware e controlli ambientali. Tali attività devono essere aggiornate periodicamente, con il risultato di ulteriori spese in conto capitale. Hanno attirato critiche perché gli utenti "devono ancora acquistarli, costruirli e gestirli" e quindi non traggono vantaggio da una gestione meno pratica, essenzialmente "[manca] il modello economico che rende il cloud computing un concetto così intrigante".

#### **A.1.8. Cloud pubblico**

*Per un confronto tra software e provider di cloud computing, consultare Confronto di cloud computing*

Un cloud viene chiamato "cloud pubblico" quando i servizi vengono resi su una rete aperta per uso pubblico. I servizi di cloud pubblico possono essere gratuiti. Tecnicamente potrebbe esserci poca o nessuna differenza tra architettura cloud pubblica e privata, tuttavia, la considerazione della sicurezza potrebbe essere sostanzialmente diversa per i servizi (applicazioni, archiviazione e altre risorse) resi disponibili da un fornitore di servizi per un pubblico pubblico e quando la comunicazione è effettuato su una rete non attendibile. In genere, fornitori di servizi di cloud pubblico come Amazon Web Services (AWS), IBM, Oracle, Microsoft, Google e Alibaba possiedono



e gestiscono l'infrastruttura nel loro data center e l'accesso avviene generalmente tramite Internet. AWS, Oracle, Microsoft e Google offrono anche servizi di connessione diretta chiamati "AWS Direct Connect", "Oracle FastConnect", "Azure ExpressRoute" e "Cloud Interconnect" rispettivamente, tali connessioni richiedono ai clienti di acquistare o affittare una connessione privata a un punto di peering offerto dal provider cloud.

### **A.1.9. Cloud ibrido**

Il cloud ibrido è una composizione di un cloud pubblico e di un ambiente privato, come un cloud privato o risorse on-premise, che rimangono entità distinte ma sono legate insieme, offrendo i vantaggi di più modelli di distribuzione. Cloud ibrido può anche significare la capacità di connettere collocazione, servizi gestiti e / o dedicati con risorse cloud. Gartner definisce un servizio cloud ibrido come un servizio di cloud computing composto da una combinazione di servizi cloud privati, pubblici e di comunità, di diversi fornitori di servizi. Un servizio cloud ibrido attraversa i confini dell'isolamento e del provider in modo che non possa essere semplicemente inserito in una categoria di servizio cloud privato, pubblico o comunitario. Consente di estendere la capacità o la capacità di un servizio cloud, mediante aggregazione, integrazione o personalizzazione con un altro servizio cloud.

Esistono vari casi d'uso per la composizione del cloud ibrido. Ad esempio, un'organizzazione può archiviare internamente dati client sensibili su un'applicazione cloud privata, ma interconnettere tale applicazione con un'applicazione di business intelligence fornita su un cloud pubblico come servizio software. Questo esempio di cloud ibrido estende le capacità dell'azienda di fornire un servizio aziendale specifico mediante l'aggiunta di servizi di cloud pubblico disponibili esternamente. L'adozione del cloud ibrido dipende da una serie di fattori come i requisiti di sicurezza e conformità dei dati, il livello di controllo necessario sui dati e le applicazioni utilizzate da un'organizzazione.

Un altro esempio di cloud ibrido è quello in cui le organizzazioni IT utilizzano risorse di cloud computing pubblico per soddisfare esigenze di capacità temporanee che non possono essere soddisfatte dal cloud privato. Questa funzionalità consente ai cloud ibridi di utilizzare il cloud bursting per il ridimensionamento tra cloud. Il cloud bursting è un modello di distribuzione di un'applicazione in cui un'applicazione viene eseguita in un cloud o data center privato e "irrompe" in un cloud pubblico quando aumenta la domanda di capacità di elaborazione. Un vantaggio principale del cloud bursting e di un modello di cloud ibrido è che un'organizzazione paga risorse di calcolo extra solo quando sono necessarie. Il cloud bursting consente ai data center di creare un'infrastruttura IT interna che supporta carichi di lavoro medi e di utilizzare risorse cloud da cloud pubblici o privati, durante picchi di richieste di elaborazione. Il modello specializzato di cloud ibrido, costruito su hardware eterogeneo, si chiama "Cloud ibrido multiplatforma". Un cloud ibrido multiplatforma è in genere alimentato da diverse architetture CPU, ad esempio x86-64 e ARM, sotto. Gli utenti possono distribuire e ridimensionare in modo trasparente le applicazioni senza conoscere la diversità hardware del cloud. Questo tipo di cloud emerge dall'aumento del sistema su chip basato su ARM per l'elaborazione di classe server.

L'infrastruttura cloud ibrida serve essenzialmente a eliminare le limitazioni inerenti alle caratteristiche di inoltro multi-accesso della rete di cloud privato. I vantaggi includono una maggiore flessibilità di runtime ed elaborazione adattiva della memoria unica per i modelli di interfaccia virtualizzati.

### **A.1.10. Altri**

#### **Community cloud**

Il cloud comunitario condivide l'infrastruttura tra diverse organizzazioni di una specifica comunità con preoccupazioni comuni (sicurezza, conformità, giurisdizione, ecc.), Gestite internamente o da terze parti e ospitate internamente o esternamente. I costi sono ripartiti su un minor numero di utenti rispetto a un cloud pubblico (ma più di un cloud privato), quindi solo una parte del potenziale di risparmio dei costi del cloud computing viene realizzato.

#### **Cloud distribuito**



Una piattaforma di cloud computing può essere assemblata da un set distribuito di macchine in posizioni diverse, connesse a una singola rete o servizio hub. È possibile distinguere tra due tipi di cloud distribuiti: elaborazione di risorse pubbliche e cloud volontario.

- **Elaborazione di risorse pubbliche:** questo tipo di cloud distribuito deriva da una definizione espansiva di cloud computing, poiché sono più simili al computing distribuito che al cloud computing. Tuttavia, è considerata una sottoclasse del cloud computing.
- **Cloud volontario:** il cloud computing volontario è caratterizzato come l'intersezione tra elaborazione di risorse pubbliche e cloud computing, in cui un'infrastruttura di cloud computing viene costruita utilizzando risorse volontarie. Molte sfide sorgono da questo tipo di infrastruttura, a causa della volatilità delle risorse utilizzate per la sua costruzione e dell'ambiente dinamico in cui opera. Può anche essere chiamato cloud peer-to-peer o cloud ad-hoc. Uno sforzo interessante in tale direzione è Cloud @ Home, che mira a implementare un'infrastruttura di cloud computing utilizzando risorse volontarie fornendo un modello di business per incentivare i contributi attraverso la restituzione finanziaria.

## Multicloud

*Articolo principale: Multicloud*

Multicloud è l'uso di più servizi di cloud computing in un'unica architettura eterogenea per ridurre la dipendenza da singoli fornitori, aumentare la flessibilità attraverso la scelta, mitigare i disastri, ecc. Si differenzia dal cloud ibrido in quanto si riferisce a più servizi cloud, piuttosto che a più implementazioni multiple modi (pubblico, privato, ereditato).

## Poly cloud

Poly cloud si riferisce all'uso di più cloud pubblici allo scopo di sfruttare servizi specifici offerti da ciascun provider. Si differenzia dal multicloud in quanto non è progettato per aumentare la flessibilità o mitigare i guasti, ma è piuttosto utilizzato per consentire a un'organizzazione di ottenere di più da fare con un singolo provider.

## Big Data cloud

I problemi legati al trasferimento di grandi quantità di dati nel cloud e alla sicurezza dei dati una volta che i dati sono nel cloud hanno inizialmente ostacolato l'adozione del cloud per i big data, ma ora che molti dati hanno origine nel cloud e con l'avvento dei server bare metal, il cloud è diventato una soluzione per casi d'uso tra cui business analytics e analisi geospaziale.

## HPC cloud

HPC cloud si riferisce all'uso di servizi e infrastrutture di cloud computing per eseguire applicazioni di elaborazione ad alte prestazioni (HPC). Queste applicazioni consumano una notevole quantità di potenza e memoria di elaborazione e vengono tradizionalmente eseguite su cluster di computer. Nel 2016 una manciata di aziende, tra cui R-HPC, Amazon Web Services, Univa, Silicon Graphics International, Sabalcore, Gcomput e Penguin Computing, hanno offerto un cloud di elaborazione ad alte prestazioni. Il cloud Penguin On Demand (POD) è stato uno dei primi servizi HPC remoti non virtualizzati offerti su base pay-as-you-go. Penguin Computing ha lanciato il suo cloud HPC nel 2016 in alternativa al cloud elastico di calcolo EC2 di Amazon, che utilizza nodi di calcolo virtualizzati.

## A.5. Architettura

L'**architettura cloud**, l'architettura dei sistemi software coinvolti nella consegna del cloud computing, in genere coinvolge più componenti cloud che comunicano tra loro tramite un meccanismo di accoppiamento libero come una coda di messaggistica. La disposizione elastica implica l'intelligenza nell'uso di accoppiamenti stretti o lenti applicati a meccanismi come questi e altri.



### A.1.11. Cloud engineering

Il **cloud engineering** è l'applicazione delle discipline ingegneristiche al cloud computing. Apporta un approccio sistematico alle preoccupazioni di alto livello di commercializzazione, standardizzazione e governance nell'ideazione, sviluppo, funzionamento e manutenzione dei sistemi di cloud computing. È un metodo multidisciplinare che comprende contributi da diverse aree come sistemi, software, web, prestazioni, ingegneria informatica, sicurezza, piattaforma, rischio e ingegneria di qualità.

## A.6. Sicurezza e privacy

### *Articolo principale: problemi di cloud computing*

Il cloud computing pone problemi di privacy poiché il fornitore di servizi può accedere ai dati presenti nel cloud in qualsiasi momento. Potrebbe alterare o eliminare accidentalmente o deliberatamente informazioni. Molti provider di servizi cloud possono condividere informazioni con terze parti, se necessario, ai fini della legge e dell'ordine senza un mandato. Ciò è consentito nelle loro politiche sulla privacy, che gli utenti devono accettare prima di iniziare a utilizzare i servizi cloud. Le soluzioni alla privacy includono politiche e normative, nonché le scelte degli utenti finali relative alla modalità di archiviazione dei dati. Gli utenti possono crittografare i dati che vengono elaborati o archiviati nel cloud per impedire l'accesso non autorizzato. I sistemi di gestione delle identità possono anche fornire soluzioni pratiche ai problemi di privacy nel cloud computing. Questi sistemi distinguono tra utenti autorizzati e non autorizzati e determinano la quantità di dati accessibili a ciascuna entità. [Citazione necessaria] I sistemi funzionano creando e descrivendo identità, registrando attività e sbarazzandosi di identità non utilizzate.

Secondo Cloud Security Alliance, le tre principali minacce nel cloud sono interfacce e API non sicure, perdita di dati e perdite e guasti hardware, che hanno rappresentato rispettivamente il 29%, il 25% e il 10% di tutte le interruzioni della sicurezza del cloud. Insieme, questi formano vulnerabilità tecnologiche condivise. In una piattaforma di provider cloud condivisa da utenti diversi potrebbe esserci la possibilità che le informazioni appartenenti a clienti diversi risiedano sullo stesso server di dati. Inoltre, Eugene Schultz, Chief Technology Officer di Emagined Security, ha affermato che gli hacker stanno spendendo molto tempo e sforzi alla ricerca di modi per penetrare nel cloud. "Ci sono dei veri tacchi di Achille nell'infrastruttura cloud che stanno facendo grandi buche per far entrare i cattivi". Poiché i dati di centinaia o migliaia di aziende possono essere archiviati su grandi server cloud, gli hacker possono teoricamente ottenere il controllo di enormi archivi di informazioni attraverso un singolo attacco, un processo che ha chiamato "hyperjacking". Alcuni esempi di questo includono la violazione della sicurezza di Dropbox e iCloud 2014. Dropbox era stato violato nell'ottobre 2014, con oltre 7 milioni di password degli utenti rubate dagli hacker nel tentativo di ottenere valore monetario da Bitcoin (BTC). Avendo queste password, sono in grado di leggere dati privati e di indicizzarli dai motori di ricerca (rendendo pubbliche le informazioni).

Esiste il problema della proprietà legale dei dati (se un utente memorizza alcuni dati nel cloud, il fornitore del cloud può trarne profitto?). Molti accordi sui Termini di servizio tacciono sulla questione della proprietà. Il controllo fisico delle apparecchiature informatiche (cloud privato) è più sicuro che avere le apparecchiature fuori sede e sotto il controllo di qualcun altro (cloud pubblico). Ciò offre un grande incentivo ai fornitori di servizi di cloud computing pubblici di dare priorità alla costruzione e al mantenimento di una solida gestione dei servizi sicuri. Alcune piccole aziende che non hanno esperienza nella sicurezza IT potrebbero scoprire che è più sicuro per loro utilizzare un cloud pubblico. Esiste il rischio che gli utenti finali non comprendano i problemi connessi all'accesso a un servizio cloud (le persone a volte non leggono le numerose pagine dei termini del contratto di servizio e fanno semplicemente clic su "Accetta" senza leggere). Questo è importante ora che il cloud computing sta diventando popolare e richiesto per far funzionare alcuni servizi, ad esempio per un assistente personale intelligente (Apple Siri o Google Now). Fondamentalmente, il cloud privato è visto come più sicuro con livelli di controllo più elevati per il proprietario, tuttavia il cloud pubblico è considerato più flessibile e richiede meno tempo e denaro da parte dell'utente.



## A.7. Limitazioni e svantaggi

---

Secondo Bruce Schneier, "Il rovescio della medaglia è che avrai opzioni di personalizzazione limitate. Il cloud computing è più economico a causa dell'economia di scala e, come qualsiasi attività esternalizzata, tendi a ottenere ciò che desideri. Un ristorante con un menu limitato è più economico di uno chef personale che può cucinare tutto quello che vuoi. Meno opzioni a un prezzo molto più economico: è una caratteristica, non un bug. " Suggerisce inoltre che "il fornitore di cloud potrebbe non soddisfare le tue esigenze legali" e che le aziende devono valutare i vantaggi del cloud computing rispetto ai rischi. Nel cloud computing, il controllo dell'infrastruttura di back-end è limitato al solo fornitore di cloud. I fornitori di servizi cloud spesso decidono in merito alle politiche di gestione, che moderano ciò che gli utenti del cloud sono in grado di fare con la loro implementazione. Gli utenti del cloud sono inoltre limitati al controllo e alla gestione delle loro applicazioni, dati e servizi. Ciò include i limiti di dati, che vengono messi sugli utenti cloud dal fornitore del cloud allocando una certa quantità di larghezza di banda per ciascun cliente e sono spesso condivisi tra altri utenti cloud.

La privacy e la riservatezza sono grandi preoccupazioni in alcune attività. Ad esempio, i traduttori giurati che lavorano secondo le disposizioni di un accordo di non divulgazione, potrebbero incontrare problemi riguardanti i dati sensibili che non sono crittografati.

Il cloud computing è vantaggioso per molte aziende; riduce i costi e consente loro di concentrarsi sulle competenze anziché sulle questioni relative a IT e infrastruttura. Tuttavia, il cloud computing ha dimostrato di avere alcune limitazioni e svantaggi, in particolare per le piccole attività aziendali, in particolare per quanto riguarda la sicurezza e i tempi di inattività. Le interruzioni tecniche sono inevitabili e si verificano a volte quando i fornitori di servizi cloud (CSP) vengono sopraffatti nel processo di servizio ai loro clienti. Ciò può comportare la sospensione temporanea dell'attività. Poiché i sistemi di questa tecnologia si basano su Internet, un individuo non può essere in grado di accedere alle proprie applicazioni, server o dati dal cloud durante un'interruzione.

## A.8. Tendenze emergenti

---

Il cloud computing è ancora oggetto di ricerca. Un fattore trainante nell'evoluzione del cloud computing sono stati i principali responsabili della tecnologia che cercavano di ridurre al minimo il rischio di interruzioni interne e mitigare la complessità della rete abitativa e dell'hardware informatico internamente. Le principali società di tecnologia cloud investono miliardi di dollari all'anno in ricerca e sviluppo nel cloud. Ad esempio, nel 2011 Microsoft ha impegnato il 90 per cento del suo budget di ricerca e sviluppo di \$ 9,6 miliardi nel suo cloud. Le ricerche condotte dalla banca d'investimento Centaur Partners alla fine del 2015 hanno previsto che le entrate di SaaS sarebbero cresciute da \$ 13,5 miliardi nel 2011 a \$ 32,8 miliardi nel 2016.