Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

Studio ed analisi sulle norme adottate per l'erogazione di servizi di Cloud Computing

Tesi di Laurea in Reti di Calcolatori

Relatore:
Chiar.mo Prof.
Fabio Panzieri

Presentata da:
Enzo Torella

Sessione III
Anno Accademico 2012/2013

Ai miei migliori amici

Indice

Introduzione

Lo scopo di questa tesi è quello di analizzare l'utilizzo del Cloud Computing ai giorni nostri come una nuova tecnologia usata da enti ed aziende, con tutti i pro e i contro, se convenga effettivamente farne uso o meno, come viene vista agli occhi di molte aziende, esaminando gli accordi giudiziari, la sicurezza e la privacy che vi sono dietro all'utilizzo di questa tecnologia e soffermandoci anche su una caratteristica principale riguardante il Cloud Computing: l'accountability. L'accountability esprime un concetto riguardante il controllo di accesso e si basa sul fatto che le parti partecipanti siano responsabili di tutto ciò che fanno all'interno del sistema; in un servizio di Cloud Computing non è semplice attribuire delle colpe in caso di perdita di dati o violazione della privacy ed è qui che viene in gioco l'accountability, aiutando le aziende ad affrontare questo tipo di problemi, soprattutto per proteggere i dati sensibili e per aumentare la fiducia degli utenti.
La tesi è strutturate in 3 capitoli.
Nel primo capitolo viene focalizzata l'attenzione sul Cloud Computing vero e proprio. Con il Cloud Computing si intende l'insieme delle infrastrutture tecnologiche in grado di elaborare, memorizzare, archiviare dati. In verità, esistono varie definizioni di Cloud Computing, ma qui si fa riferimento alla definizione data dal NIST (National Institute of Standards and Technology): il Cloud è un ambiente di esecuzione sulla rete che permette la condivisione di risorse di calcolo. Vengono evidenziate le principali caratteristiche del Cloud, ossia:

- L'elasticità: è possibile fornire e rilasciare risorse in qualsiasi momento e quantità.

- Controllo sui servizi: il fornitore del servizio di Cloud controlla le richieste pervenute.

- Self-service su richiesta: il cliente può porre dei vincoli sull'uso del servizio.

- Accesso alle risorse su banda larga

- Risorse comuni: il provider del servizio mette a disposizione del cliente le risorse in modo dinamico.

Una caratteristica che rende peculiare l'utilizzo del Cloud Computing è la virtualizzazione. Con questa è possibile astrarre l'hardware e renderlo disponibile in forma virtuale in modo da poter installare sistemi operativi.
Con la virtualizzazione si hanno server più affidabili e flessibili, vi è un risparmio di tempo, una diminuzione nei costi di gestione e manutenzione, riduzione del numero di server; così tutto ciò consente di investire nel Cloud Computing.
In base al tipo di servizio richiesto si possono distinguere tre modelli di Cloud Computing:

- Infrastructure as a Service (Iaas): Iaas consiste in un'infrastruttura di risorse hardware che comprende una moltitudine di server e dati, distribuite su svariati data center.

- Platform as a Service (Paas): Paas è un modello di Cloud Computing che fornisce un'interfaccia di programmazione (API) per consentire agli utenti di creare applicazioni e servizi su Internet e sono accessibili dagli utenti semplicemente tramite il loro browser. Le Paas permettono agli utenti di creare applicazioni software utilizzando gli strumenti forniti dal provider.

- Software as a Service (Saas): Saas è un modello di servizio i cui clienti possono accedere alle applicazioni software su Internet e viene spesso definito come "software on demand" e l'utilizzo è simile al noleggio del software che all'acquisto.

Il Cloud Computing si divide in Hybrid Cloud, Public Cloud e Private Cloud.

- Per Private Cloud si intende un particolare modello di Cloud Computing in cui solo il cliente specificato può operare ed egli opererà solo all'interno di un ambiente virtualizzato. Secondo questo modello di Cloud, il servizio è accessibile solo da una singola organizzazione che detiene maggior controllo e privacy.

- Per Hybrid Cloud si fa riferimento ad un servizio di Cloud integrato che utilizza sia Public che Private Cloud per svolgere funzioni distinte all'interno della stessa organizzazione, in modo da massimizzare la propria efficienza di utilizzo.

- Per Public Cloud si intende un modello di Cloud col quale i servizi vengono forniti in ambiente virtualizzato. Esso fornisce anche servizi a più clienti utilizzando la stessa infrastruttura condivisa.

Con il Cloud Computing vi è una diminuzione nei costi, memorizzazione dei dati illimitata, ripristino e backup dei dati, facile accesso alle informazioni. Ma con esso vi sono anche degli svantaggi: a volte il sistema può avere dei malfunzionamenti durante l'utilizzo del servizio; la memorizzazione di dati privati può rendere vulnerabile la sicurezza di un'azienda la quale può essere soggetta ad attacchi esterni.
A volte spesso si fa confusione tra Cloud e Grid Computing. Sono simili ma con qualche piccola differenza: mentre nel Cloud vi è un singolo provider che fornisce a più organizzazioni le risorse per l'esecuzione di applicazioni simili, nel Grid Computing vi è la condivisione di risorse all'interno di una organizzazione dinamica virtuale.
Nel secondo capitolo viene data una panoramica sugli SLA (Service Level Agreement). Per SLA si intende un accordo stipulato tra un provider di servizi ed il suo cliente per poter usufruire al meglio del servizio. Qui l'attenzione viene focalizzata su un'architettura per la

virtualizzazione delle risorse basata sugli SLA che fornisce una soluzione per l'esecuzione di applicazioni nel Cloud. Questo lavoro rappresenta il primo tentativo di combinare le negoziazioni di risorse basate su SLA con risorse virtualizzate in termini di fornitura di servizi on-demand. L'architettura SRV si basa su tre elementi principali: il contratto di negoziazione, il servizio di brokering e l'implementazione del servizio.

Per quanto riguarda il contratto di negoziazione, prima di impegnarsi a sottoscrivere un SLA, l'utente e il provider decidono quali parametri adottare e le sanzioni nel caso in cui uno di loro violi un SLA. Per quanto concerne il servizio di brokering, se il servizio richiesto viene trovato, il documento SLA verrà accettato, altrimenti sarà rifiutato. Invece per quanto riguarda l'implementazione del servizio, dopo che le parti partecipanti si siano messe d'accordo sui requisiti del servizio e abbiano accettato il SLA, il servizio può finalmente esser implementato tramite la virtualizzazione.

Nel terzo capitolo l'attenzione si focalizza sulla sicurezza, la privacy e l'accountability. Utilizzando un servizio di Cloud Computing vi sono dei problemi riguardo alla sicurezza dei dati, dovuti ad applicazioni maligne che girano nel Cloud. Le aziende così hanno dovuto rendere anonimi i loro dati. Dato che gli ambienti Cloud cambiano molto rapidamente, le aziende devono cercare sempre di mantenere degli standard di sicurezza conformi; si cerca, quindi, di progettare servizi Cloud in grado di ridurre il rischio di violazione della privacy. Il fatto che le persone ottengano un accesso non autorizzato ai dati personali nel Cloud, sfruttando alcune vulnerabilità come la mancanza di procedimenti di controllo agli accessi, può costituire una seria minaccia alla privacy. Per ridurre i rischi di violazione della privacy ci devono essere lealtà e trasparenza tra coloro che utilizzano un servizio di Cloud, ed inoltre il consenso da parte degli utenti affinché i loro dati possano essere usati per determinati scopi; solo le informazioni necessarie a soddisfare lo scopo prefissato devono essere raccolte e condivise in modo da ridurre l'utilizzo di informazioni personali. Devono esserci, altresì, determinate misure di sicurezza per impedire l'accesso non autorizzato ed anche una persona responsabile per assicurare che le norme sulla privacy vengano rispettate. Un servizio deve predisporre di funzioni di audit per monitorare gli accessi. Cosi, le aziende cercano di adottare meccanismi per gestire i dati in modo responsabile. L'accountability sembra essere un approccio allettante e viene adottato tramite misure volte a collegare politiche di sicurezza e privacy ai dati, in modo che vengano rispettate tali politiche. In un

sistema che fa uso di accountability deve essere possibile rilevare ogni errore, bisogna tenere traccia di ogni azione compiuta dagli utenti in modo da risalire al colpevole in caso di anomalie tramite un auditor.

Capitolo 1: Cloud Computing

1.1 Il Cloud Computing

Con il concetto di Cloud Computing ("nuvola informatica" in inglese) viene designato l'insieme di infrastrutture tecnologiche in grado di elaborare, archiviare, memorizzare dati grazie all'utilizzo di risorse hardware/software tramite un servizio di client/server. Secondo l'ENISA (European Network and Information Security Agency) il Cloud Computing è un nuovo approccio di erogazione di servizi IT, non una nuova tecnologia [1].
Esistono varie definizioni di Cloud Computing, ma facciamo riferimento a quella proposta dal NIST (National Institute of Standards and Technology):

"Cloud computing is a model of enabling convenient, on demand network access to shared pool of configurable computing resources (e.g. networks, servers, storage, applications and service) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]".

Il Cloud Computing ha molte caratteristiche, ma il NIST ne prende a fuoco cinque [2]:

1) **Elasticità:** le risorse vengono fornite in modo più rapido e l'utente ne può richiedere quante ne vuole e in qualsiasi momento.
2) **Controllo sui servizi:** il fornitore, per garantire la qualità del servizio al cliente, deve monitorare l'utilizzo del servizio in modo da evitare il sovrabbondare di richieste.
3) **Self-service su richiesta:** il cliente può richiedere dei vincoli sull'utilizzo del servizio, senza chiedere un aiuto esterno da parte del fornitore.

[1] "Il Cloud Computing è un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio rete, server, dispositivi di memorizzazione, applicazioni e servizi) sotto forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore."

4) **Accesso a banda larga:** è possibile accedere alle risorse tramite la rete, con l'uso di piattaforme client.
5) **Risorse comuni:** a seconda della richiesta da parte del cliente, le risorse vengono assegnate dinamicamente in modo da servire più clienti. Il cliente non conosce l'esatta posizione delle risorse a cui vuole accedere, ma il fornitore può decidere se il cliente può specificare dei vincoli sulla posizione delle risorse, come il Paese o lo specifico data center. Esempi di queste risorse sono: macchine virtuali,risorse di calcolo ecc…

Altre caratteristiche comuni sono:

1) **la virtualizzazione:** consiste nell'astrarre le componenti hardware e di renderle disponibili in forma virtuale su cui è possibile installare poi sistemi operativi. La virtualizzazione rende un servizio più dinamico, offrendo agli utenti un nuovo modo di archiviare ed elaborare dati ed essa sta alla base del Cloud Computing. I suoi principali vantaggi sono:
   - server più affidabili e flessibili; in caso di guasti o problemi di varia natura è possibile continuare il lavoro.
   - rispiarmo di tempo.
   - diminuzione nei costi di gestione e manutenzione; ciò consente di investire nel Cloud Computing e in nuove tecnologie.
   - riduzione del numero di server; è possibile aggiungere nuovi database [3].
2) **pagamento in base all'utilizzo dei servizi:** il cliente sceglie il fornitore ed il rispettivo servizio a seconda delle proprie esigenze, e può richiedere l'utilizzo delle risorse dinamicamente, ossia quando e per quanto tempo vuole. Il cliente successivamente pagherà solo in base all'effettivo sfruttamento delle risorse. Questa caratteristica consente al cliente di ridurre il numero di risorse presenti nelle sue strutture, notificando al fornitore le risorse non utilizzate.

1.2 Modelli di servizio

In base al tipo di servizio richiesto, si possono distinguere vari tipi di servizi di Cloud Computing i quali posso essere implementati utilizzando risorse comuni offerti da un fornitore ai propri clienti oppure risorse dedicate ad un unico cliente. Il cliente, in base alle proprie esigenze, sceglierà il tipo di servizio. Di seguito elenchiamo tre modelli principali di servizi di Cloud Computing dal livello hardware al livello applicativo.

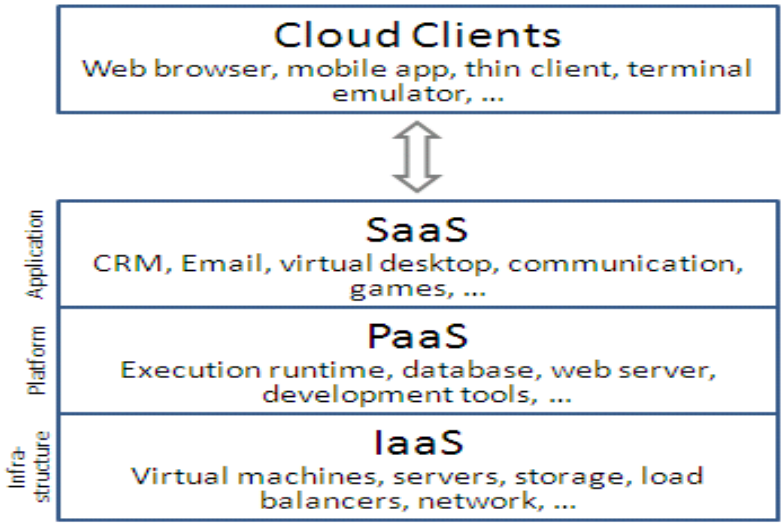

Figura 1 - Modelli di Servizio del Cloud Computing [4]

1.2.1 Infrastructure as a Service (IaaS)

Iaas è un modello che consiste in un'infrastruttura con capacità di memorizzazione e di rete sul quale il cliente può costruire le proprie piattaforme IT. Fisicamente, l'insieme delle risorse hardware comprende una moltitudine di server e reti di solito distribuite su numerosi data center. Questo modello può essere utilizzato dai clienti aziendali per creare soluzioni IT facilmente scalabili, dove le complessità e le spese di gestione dell'hardware sottostante sono esternalizzate al cloud provider. Se la scala delle operazioni di un cliente aziendale fluttua, o i clienti stanno cercando di espandersi, possono attingere alla risorsa Cloud, come e quando ne hanno bisogno, piuttosto che acquistare, installare e integrare hardware a se stessi.

I seguenti sono esempi salienti di come le IaaS possono essere utilizzate dalle aziende:

- **Cloud hosting;** un sito web “ospitato” in un servizio di Cloud opera su diversi server connessi fra loro, a differenza del server singolo tradizionale. Si ha cosi una potenza di calcolo virtualmente infinita che può crescere a seconda delle esigenze dell’utente, aggiungendo altri server al cluster. In caso di guasti di uno dei macchinari, gli altri faranno da “sostituti” senza interrompere il servizio.

- **Virtual Data Centers (VDC);** una rete virtuale che può offrire funzionalità di Cloud hosting e che può integrare numerose operazioni all’interno sia di un’implementazione di Cloud privato che di Cloud pubblico.

Una tipica Iaas può beneficiare delle seguenti caratteristiche:

- **Scalabilità:** l’infrastrutture Iaas consente di aumentare e diminuire le risorse dei singoli Cloud server in tempo reale.

- Nessun investimento in hardware; l'hardware fisico sottostante che supporta un servizio IaaS è mantenuto dal fornitore del Cloud, risparmiando il tempo e il costo di tale operazione sul lato client.

- il servizio è accessibile su richiesta e il cliente paga solo per le risorse che effettivamente usa

- Al servizio è possibile accedere da ogni luogo purchè vi sia una connessione e il protocollo di sicurezza del Cloud lo permetta.

- **Nessun guasto;** se un server dovesse guastarsi il servizio in generale rimarrebbe inalterato a causa della moltitudine di risorse hardware. Per molti servizi, se un intero data center dovesse andare offline, il servizio IaaS potrebbe ancora funzionare correttamente.

1.2.2 Platform as a Service (Paas)

Paas è un modello di Cloud Computing che fornisce un'interfaccia di programmazione (API) per consentire agli utenti di creare applicazioni e servizi su Internet. I servizi PaaS sono "ospitati" nel Cloud e accessibili dagli utenti semplicemente tramite il loro browser.
Le Paas permettono agli utenti di creare applicazioni software utilizzando gli strumenti forniti dal provider. Nei servizi Paas sta al cliente scegliere quali caratteristiche soddisfino le proprie esigenze e scartare quelle che non le soddisfino.
I servizi sono costantemente aggiornati, con le caratteristiche esistenti aggiornate e funzionalità aggiunte. I fornitori PaaS possono supportare i clienti dalla concezione delle loro idee originali per la creazione di applicazioni fino al collaudo e la distribuzione. Tutto ciò si ottiene con un meccanismo gestito.
Qui di seguito elenchiamo alcune delle caratteristiche che possono essere incluse in un servizio Paas:

- Sistema operativo
- Ambiente di scripting server-side
- Sistema di gestione di database
- Software Server
- Memorizzazione di dati
- Accesso alla rete
- Strumenti per la progettazione e lo sviluppo
- Hosting

Gli sviluppatori software, sviluppatori web e le aziende possono beneficiare di PaaS. Ad esempio gli sviluppatori web possono utilizzare ambienti singoli PaaS in ogni fase del processo per sviluppare, testare e infine "ospitare" i loro siti web.
Elenchiamo alcuni dei vantaggi di Paas per gli sviluppatori di applicazioni:

- **Non c'è bisogno di investire in infrastrutture fisiche**; adottando un'infrastruttura virtuale si hanno vantaggi economici e pratici. Non c'è bisogno di acquistare hardware. Questo lascia liberi di concentrarsi sullo sviluppo di applicazioni.

- **Rende lo sviluppo possibile per i 'non esperti'**; con PaaS chiunque può sviluppare un'applicazione. Si può semplicemente farlo attraverso il proprio browser utilizzando le funzionalità con un solo clic. Un esempio è WordPress[2].

- **Flessibilità;** i clienti possono avere il controllo sugli strumenti che vengono installati all'interno delle loro piattaforme e creare applicazioni che si adattino alle loro esigenze.

- **Adattabilità;** le caratteristiche possono essere modificate se le circostanze lo impongono.

- **Team di ogni luogo possono lavorare insieme;** dotati di una connessione ad internet e di un browser, sviluppatori di diverse sedi possono lavorare insieme sulla stessa applicazione.

- **Sicurezza;** viene fornita la sicurezza dei dati, inclusi il backup e il ripristino.

In sostanza, il Paas fornisce l'architettura e l'infrastruttura per supportare lo sviluppo di applicazioni. Questo include servizi di rete, di memorizzazione, di supporto e di gestione del software. È quindi ideale per lo sviluppo di nuove applicazioni che sono destinate al web così come i dispositivi mobili.

1.2.3 Software as a Service (Saas)

Il Saas[4] descrive qualsiasi servizio di Cloud in cui i consumatori sono in grado di accedere alle applicazioni software in rete. Le applicazioni sono “ospitate” nella "nuvola" e possono essere utilizzate per una serie di attività sia per gli individui e le organizzazioni. Google, Twitter e Facebook sono tutti esempi di SaaS, con gli utenti in grado di accedere ai servizi

[2] WordPress è una piattaforma software di “personal publishing” e content management system (CMS), sviluppata in PHP e che usa come database MySQL. Consente la creazione di un sito internet formato da contenuti testuali

tramite qualsiasi dispositivo abilitato a Internet. Gli utenti aziendali sono in grado di utilizzare le applicazioni per una serie di esigenze, tra cui la contabilità e la fatturazione, le vendite di monitoraggio, pianificazione, monitoraggio delle prestazioni e delle comunicazioni (comprese le e-mail e messaggi istantanei).
Saas è spesso definito come "software on demand" e l'utilizzo è simile al noleggio del software che all'acquisto. Con le applicazioni software tradizionali si desidera acquistare il software come un pacchetto e poi installarlo. La licenza del software può inoltre limitare il numero di utenti. Gli utenti Saas effettuano un abbonamento al software piuttosto che acquistarlo, di solito su base mensile.
Ci sono una serie di motivi per cui SaaS è vantaggioso per le organizzazioni e gli utenti:

- **Nessun costo hardware aggiuntivo;** la potenza di elaborazione necessaria per eseguire le applicazioni è fornita dal provider del Cloud.

- **Nessun costo di installazione iniziale;** le applicazioni sono pronte da usare una volta che gli utenti si siano abbonati al servizio.

- **Si paga per ciò che viene utilizzato;** se il software è utilizzato per un breve periodo si paga solo per quel periodo e l'abbonamento può essere disdetto in qualsiasi momento.

- **L'uso è scalabile;** se un utente ha bisogno di più spazio di archiviazione o servizi aggiuntivi, per esempio, allora può accedere a questi "on demand" senza la necessità di installare nuovo software o hardware.

- **Gli aggiornamenti sono automatici;** ogni qualvolta che c'è un aggiornamento, esso è disponibile on-line per i clienti, spesso gratuitamente. Nessun nuovo software sarà richiesto come spesso accade con altri tipi di applicazioni e gli aggiornamenti di solito saranno distribuiti automaticamente dal provider del Cloud.

- **Compatibilità cross-device;** si può accedere alle applicazioni SaaS tramite qualsiasi dispositivo abilitato a Internet, il che lo rende ideale per chi utilizza un certo numero di dispositivi diversi.

- **Accesso da qualsiasi luogo;** piuttosto che essere limitata alle installazioni su ogni computer, si può accedere ad un'applicazione da qualsiasi luogo tramite un dispositivo abilitato a Internet.

- **Le applicazioni possono essere personalizzate;** tramite alcuni software, un'applicazione può essere modificata per soddisfare le esigenze di un particolare cliente.

Compiti relativi alla contabilità, fatturazione, vendite e pianificazione possono essere eseguite tramite Software as a Service. Le aziende potrebbero voler utilizzare un tipo di software che esegua tutti questi compiti. Il software necessario a fare ciò può essere sottoscritto via Internet e quindi accessibile on-line tramite un qualsiasi computer in ufficio utilizzando un nome utente e una password. Se le esigenze cambiano si può facilmente passare a software che soddisfi le proprie esigenze. Chiunque voglia accedere ad un particolare tipo di software può essere registrato come utente.

1.3 Modelli di erogazione

Sempre in base alla definizione proposta dal NIST, il Cloud si divide in:

- Private Cloud
- Public Cloud
- Hybrid Cloud

1.3.1 Private Cloud

Un Cloud privato è un particolare modello di Cloud Computing che coinvolge un ambiente di Cloud distinto e sicuro in cui solo il cliente specificato può operare. Come altri modelli di Cloud, il Cloud privato opererà all'interno di un ambiente virtualizzato utilizzando una base di risorse fisiche. Tuttavia, secondo il modello di Cloud privato, la "nuvola" è accessibile solo da una singola organizzazione che detiene maggiore controllo e privacy.
I meccanismi tecnici utilizzati per fornire i diversi servizi che possono essere classificati come servizi di Cloud privato variano notevolmente e quindi è difficile definire ciò che costituisce un Cloud privato dal punto di vista tecnico. Invece tali servizi sono di solito classificati in base alle caratteristiche che essi offrono ai loro clienti. Tratti salienti che caratterizzano il Cloud privato sono l'uso esclusivo della "nuvola" da parte di un'azienda e più elevati livelli di sicurezza della rete. Essi possono essere in contrasto con un Cloud pubblico che ha più clienti che accedono ai servizi virtualizzati, cui tutti traggono le loro risorse dallo stesso insieme di server attraverso le reti pubbliche. I servizi di Cloud privato traggono le proprie risorse da un insieme distinto di server, ma questi possono essere "ospitati" internamente o esternamente e si può accedere attraverso rete privata o garantendo connessioni crittografate tramite reti pubbliche.
Il Cloud privato è stato concepito per le aziende che vogliono maggior controllo sui dati. Il modello di Cloud privato è più vicino al modello più tradizionale delle reti ad accesso locale (LAN) utilizzate in passato dalle imprese, ma con il vantaggio aggiunto della virtualizzazione. Le caratteristiche e i vantaggi del Cloud privato sono quindi:

- **Maggior sicurezza e privacy;** i servizi di Cloud pubblico possono implementare un certo livello di sicurezza, ma quelli di Cloud privato - utilizzando tecniche come insiemi distinti di risorse con accesso limitato alle connessioni dietro ad un firewall- sono in grado di garantire che le operazioni siano tenute alla larga da occhi indiscreti.

- **Più controllo;** visto che un Cloud privato è accessibile solo da una singola organizzazione, tale organizzazione avrà la possibilità di configurare e gestire in linea con le proprie esigenze il servizio per realizzare una soluzione di rete su

misura. Tuttavia, questo livello di controllo rimuove le cosiddette economie di scala generate nel Cloud pubblico così da avere una gestione centralizzata dell'hardware.

- **Il cloud bursting;** esso è una funzionalità che consente all'impresa di mediare e gestire la fornitura dei servizi tra più Cloud a partire da un unico punto di controllo integrato. Il bursting permette all'impresa di integrare le proprie risorse locali con quelle originate da altri Cloud provider per soddisfare richieste di maggiore capacità, ampliare la copertura geografica o sfruttare offerte di infrastruttura specializzate. In un Cloud privato, quindi, alcuni provider possono offrire la possibilità di utilizzare il Cloud bursting in caso di picchi di domanda in modo da far migrare l'esecuzuone dei workload in un Cloud pubblico [5].

1.3.2 Public Cloud

Il modello più conosciuto di Cloud Computing per molti consumatori è il modello di Cloud pubblico, in base al quale i servizi Cloud sono forniti in ambiente virtualizzato, realizzato utilizzando un insieme di risorse fisiche condivise e accessibili attraverso una rete pubblica. I Cloud pubblici, tuttavia, forniscono servizi, anche in maniera gratuita, a più client utilizzando la stessa infrastruttura condivisa.
Gli esempi più salienti del Cloud Computing tendono a cadere nel modello di Cloud pubblico, perché sono, per definizione, a disposizione del pubblico. Software as a Service (SaaS) e applicazioni da ufficio online sono forse i più familiari, ma anche Infrastructure as a Service (IaaS) e Platform as a Service (PaaS), tra cui il Cloud basato sul web hosting (anche se tutti possono esistere anche all'interno di Cloud privati).
Il modello pubblico offre le seguenti caratteristiche e vantaggi:

- **Costo efficace;** i Cloud pubblici comprendono maggiori livelli di risorse e quindi possono beneficiare di maggiori economie di scala. Il funzionamento e la gestione delle risorse di base è condivisa in tutti i successivi servizi di Cloud.

- **pay-as-you-go;** i servizi di Cloud pubblici spesso impiegano un modello pay-as-you-go in base al quale il consumatore sarà in grado di accedere alla risorsa di cui ha bisogno, quando ne ha bisogno, e poi pagare solo ciò che utilizza, evitando così spreco di capacità.

- **Affidabilità;** non c'è nessun rischio di errore che renderebbe un servizio di Cloud pubblico vulnerabile.

- **Flessibilità;** ci sono una miriade di servizi di tipo IaaS, PaaS e SaaS disponibili sul mercato che seguono il modello di Cloud pubblico e che si può loro accedere da qualsiasi dispositivo abilitato a Internet. Questi servizi possono soddisfare la maggior parte delle esigenze di calcolo e in grado di fornire benefici a clienti privati e aziendali. Le aziende possono anche integrare i loro servizi di Cloud pubblico con quelli di Cloud privato, dove si ha il bisogno di svolgere funzioni aziendali delicate, per creare Cloud ibridi.

- **Indipendenza dal luogo in cui ci si trova;** grazie ad una connessione i servizi sono disponibili ovunque il cliente si trovi. Questo fornisce per esempio l'accesso remoto alle infrastrutture IT (in caso di emergenze, ecc).

1.3.3 Hybrid Cloud

Un Cloud ibrido è un servizio di Cloud integrato che utilizza i Cloud pubblici e privati per svolgere funzioni distinte all'interno della stessa organizzazione. Tutti i servizi di Cloud Computing dovrebbero offrire alcune efficienze a livelli diversi ma i servizi di Cloud pubblico rischiano di essere più convenienti di quelli di Cloud privato. Pertanto, un'organizzazione può massimizzare la propria efficienza utilizzando servizi di Cloud pubblico per tutte quelle operazioni non delicate, basandosi solo su un Cloud privato dove si richiede che tutte le proprie piattaforme siano perfettamente integrate.

I modelli di Hybrid Cloud possono essere implementati in diversi modi:

- Diversi team di Cloud provider per fornire sia servizi pubblici e privati come servizio integrato.

- Fornitori di ogni Cloud offrono un pacchetto ibrido completo .

- Le aziende che gestiscono i loro Cloud privati si iscrivono ad un servizio di Cloud pubblico che poi integrano nella loro infrastruttura.

In pratica, un'organizzazione potrebbe implementare un Cloud ibrido per ospitare il proprio sito e-commerce all'interno di un Cloud privato, dove vi è più sicurezza, e il proprio brochure site[3] in un Cloud pubblico. In alternativa, l'Infrastructure as a Service (IaaS), per esempio, potrebbe seguire il modello di Cloud ibrido e fornire una struttura finanziaria con una memoria per i dati del cliente all'interno di un Cloud privato, ma poi consentire la collaborazione sui documenti di pianificazione del progetto nel Cloud pubblico, dove possono accedere più utenti da qualsiasi postazione.
Un Cloud ibrido è in grado di offrire ai suoi utenti le seguenti caratteristiche:

- **Scalabilità;** spostando molte funzioni non delicate al Cloud pubblico consente a un'organizzazione di beneficiare della scalabilità del Cloud pubblico riducendo le richieste su un Cloud privato.

- **Efficienze nei costi;** il Cloud pubblico è in grado di offrire una maggiore efficienza nei costi rispetto al Cloud privato. I Cloud ibridi permettono quindi alle aziende di risparmiare.

[3] Il brochure site è un sito che pubblicizza il prodotto di un'azienda e migliora i propri sforzi di vendita e marketing

- **Sicurezza;** la componente privata del modello di Cloud ibrido non solo fornisce la sicurezza per le operazioni delicate, ma può anche soddisfare i requisiti normativi per la gestione e la memorizzazione dei dati.

- **Flessibilità;** si possono fornire risorse in tempo reale.

1.4 Benefici e rischi del Cloud Computing

Elenchiamo una serie di vantaggi e svantaggi riguardanti il Cloud Computing.

1.4.1 Vantaggi e benefici del Cloud Computing

Diminuzione nei costi

Il più grande vantaggio del Cloud computing è l'eliminazione dell'investimento in software da parte dell'utente. Con il Cloud computing si può facilmente risparmiare nelle spese generali come il costo di archiviazione dei dati, aggiornamenti software, gestione, e soprattutto il costo del controllo di qualità. Ora chiunque può utilizzare i servizi di Cloud Computing a prezzi accessibili. Il Cloud Computing è probabilmente il metodo più efficiente per utilizzare, mantenere e aggiornare. Alcuni software tradizionali costano alle aziende un sacco in termini di finanza. Sommando i costi di licenza per più utenti può rivelarsi molto costoso per l'azienda in questione. Il Cloud, invece, è disponibile a prezzi molto più economici e, quindi, in grado di ridurre in modo significativo le spese IT dell'azienda. Inoltre, ci sono molte opzioni scalabili tra cui il pay-as-you-go, che lo rende molto conveniente per l'azienda in questione.

La velocità e la scalabilità dei servizi di Cloud Computing

Con il Cloud Computing, il cliente non ha bisogno di installare hardware o software per una nuova applicazione. Ci sono molti data center che si trovano in più sedi per la memorizzazione dei dati.

Memorizzazione quasi illimitata

La memorizzazione delle informazioni nel Cloud ti dà la possibilità di archiviare i dati in maniera praticamente illimitata. Quindi, non è più necessario preoccuparsi di rimanere a corto di spazio di archiviazione o di aumentare la memoria attuale.

Ripristino e backup

Poiché tutti i dati sono memorizzati nel Cloud, eseguendo il backup e il ripristino è relativamente molto più facile del memorizzare i dati stessi su un dispositivo fisico. Inoltre, la maggior parte dei fornitori di servizi di Cloud, di solito, sono abbastanza competenti nel recuperare le informazioni. Quindi, questo rende l'intero processo di backup e ripristino molto più semplice di altri metodi tradizionali di memorizzazione dei dati.

Integrazione di software automatico

Nel Cloud, l'integrazione del software di solito è una cosa che avviene automaticamente. Questo significa che non è necessario fare ulteriori sforzi per personalizzare e integrare le applicazioni secondo le proprie esigenze. Quindi, si possono scegliere solo quei servizi e applicazioni software che si pensa possano soddisfare al meglio le proprie esigenze.

Facile accesso alle informazioni

Una volta che l'utente si è registrato nel servizio di Cloud, può accedere alle informazioni da qualsiasi luogo. Questa caratteristica lo lascia libero di vedere con buon occhio oltre il fuso orario e le questioni di posizione geografica.

Rapido funzionamento

Il Cloud Computing offre il vantaggio di funzionamento rapido. Una volta che si opta per questo metodo di funzionamento, l'intero sistema può essere pienamente funzionante nel giro di pochi minuti. Naturalmente, la quantità di tempo impiegato qui dipenderà dal tipo esatto di tecnologia di cui si ha bisogno per il proprio lavoro.

Innovazione nella tecnologia

Con l'innovazione nella tecnologia, il cliente non ha bisogno di gestire le proprie risorse; il Cloud Computing fa tutto questo e fornisce al cliente i benefici completi.

Selezione della locazione

I fornitori di servizi possono selezionare la locazione per le infrastrutture liberamente, secondo le proprie esigenze, riducendo al minimo le spese generali.

Utilizzo di qualsiasi dispositivo

Si può accedere ai servizi di Cloud Computing da qualsiasi dispositivo.

Miglior flusso di cassa

Se si opta per un servizio di Cloud pubblico o Cloud privato, il Cloud Computing fornisce un migliore flusso di cassa, eliminando le spese di capitale associato alla costruzione delle infrastrutture server.

Distribuzione di progetti con maggior velocità: dial-up[4]

Poiché i server possono essere distrutti in pochi minuti, il tempo per distribuire una nuova applicazione viene minimizzato con il Cloud Computing. Invece di installare un nuovo server , il nuovo server può essere connesso alla rete attraverso una console di controllo. O meglio ancora, con un Cloud privato, il provider di servizi può collegare un nuovo server alla rete eseguendo una singola chiamata.

Scalabilità

Visto che le applicazioni possono aver bisogno di spazio, è possibile aggiungere memoria, se necessario. Ciò significa che è possibile acquistare "il minimo indispensabile" in base a ciò che serve per l'applicazione.

[4] Con dial-up si fa riferimento alle connessioni tra computer realizzate con l'utilizzo di modem tramite la composizione di una normale numerazione telefonica, cioè dunque utilizzando l'usuale banda fonica a bassa frequenza, grazie a opportuni programmi detti dialer.

Minor costi di manutenzione

Minor costi di manutenzione per quanto concerne l'hardware. Visto che il Cloud Computing utilizza meno risorse fisiche, c'è meno hardware da mantenere.

Maggior efficacia riguardante la collaborazione

Il Cloud Computing aumenta la collaborazione consentendo a tutti i dipendenti - ovunque si trovino - di sincronizzare e lavorare simultaneamente su documenti e applicazioni condivise, e seguire i colleghi e le registrazioni per ricevere gli aggiornamenti critici in tempo reale. Un sondaggio condotto da Frost & Sullivan ha scoperto che le aziende che hanno investito nella tecnologia di collaborazione hanno avuto un rendimento del 400% sull'investimento.

Lavorare da qualsiasi luogo

Fintanto che i dipendenti hanno accesso alla rete, possono lavorare da qualsiasi luogo. Questa flessibilità influisce positivamente sulla produttività.

Sicurezza

Circa 800.000 computer portatili vengono persi ogni anno negli aeroporti. Questo può avere alcune gravi implicazioni monetarie, ma quando tutto è memorizzato nel Cloud, i dati possono ancora essere recuperati.

Competitività

Uno studio ha scoperto che le aziende che non hanno utilizzato il Cloud hanno dovuto affidarsi a metodi di backup su nastro e a procedure complicate per il recovery.

Ambiente pulito

Le aziende che adottano il Cloud Computing utilizzano solo lo spazio server di cui hanno bisogno, il che riduce le emissioni di carbonio. Utilizzando il Cloud si ha almeno il 30% in

meno di consumo energetico ed emissioni di anidride carbonica rispetto all'utilizzo di server. E ancora, le PMI[5] ottengono il massimo beneficio.

La diversità dei dispositivi

Si può accedere al Cloud tramite vari dispositivi elettronici differenti che sono in grado di collegarsi ad Internet. Questi dispositivi includono iPad, smartphone, laptop o computer da tavolo.

Impostazioni personalizzate

Ultimo ma non meno importante, è possibile personalizzare le applicazioni aziendali con il Cloud. Questo è un grande vantaggio perché il mondo del business online è molto competitivo.

1.4.2 Svantaggi e rischi del Cloud Computing

Problemi tecnici

Anche se è vero che si può accedere alle informazioni ed ai dati nel Cloud in qualsiasi momento e da qualsiasi luogo, ci sono momenti in cui questo sistema può avere qualche malfunzionamento. È necessario essere consapevoli del fatto che questa tecnologia è sempre soggetta a problemi tecnici. Anche i migliori fornitori di servizi di Cloud possono incorrere in questo tipo di problemi, nonostante abbiano adottato elevati standard di manutenzione. Inoltre, si avrà bisogno di una buona connessione ad Internet per essere registrati sui server in qualsiasi momento. Ci può essere il problema di rimanere sempre bloccati in caso di problemi di rete e connettività.

Sicurezza nel Cloud

Prima di adottare questa tecnologia, si dovrebbe sapere che si daranno informazioni riservate dell'azienda ad un provider di servizi di Cloud di terze parti. Questo metterebbe l'azienda a grande rischio. Quindi, è necessario essere assolutamente sicuri di scegliere il fornitore di servizi più affidabile, che cercherà di tenere i dati totalmente al sicuro.

[5] PMI sta per piccole e medie imprese.

Soggetto ad attacchi

La memorizzazione delle informazioni nel Cloud potrebbe rendere l'azienda vulnerabile agli attacchi di hacker esterni e ad altri tipi di minacce. Come ben si sa, niente sulla rete è completamente al sicuro e, quindi, c'è sempre il rischio del "furto" dei dati sensibili.

1.5 Grid Computing

Il Grid Computing è una forma di calcolo distribuito che coinvolge il coordinamento e la condivisione di calcolo, applicazioni, dati e archiviazione o risorse di rete attraverso un'organizzazione dinamica e geograficamente sparsa[6]. Le tecnologie del Grid Computing promettono di cambiare il modo delle organizzazioni di affrontare alcuni problemi computazionalmente complessi. La visione del Grid Computing era quella di consentire l'accesso alle risorse del computer (da cicli di CPU ai dati server) [7, 8, 9]. Questo ha dato luogo all'idea dei Virtual Organizations (VO). Attraverso la realizzazione dei VO, era possibile accedere a tutte le risorse come se fossero tutte di proprietà di una singola organizzazione. Vi sono nel Grid due risultati-chiave: the Open Grid Service Architecture (OGSA)[6] [10] e il Globus Toolkit[7] [11].

1.5.1 Caratteristiche del Grid Computing

Lavorare su larga scala

Un servizio di Grid Computing deve essere in grado di aver a che fare con una serie di risorse che possono essere poche o più di un milione. Questo pone il problema di evitare il potenziale degrado delle prestazioni appena la dimensione del servizio aumenta.

Distribuzione geografica

Le risorse possono essere localizzate in posti diversi.

[6] OGSA descrive un'architettura di Grid Computing per uso scientifico e aziendale
[7] Il Globus Toolkit è un toolkit open source per sviluppare sistemi Grid, sviluppato e fornito da Globus Alliance

Eterogeneità

Un servizio di Grid Computing ospita sia risorse software e hardware che possono variare dai dati, file, componenti software a strumenti scientifici, dispositivi di visualizzazione, agende personali digitali e reti.

La condivisione delle risorse

Le risorse in un servizio di Grid appartengono a diverse organizzazioni che permettono ad altre organizzazioni (ad esempio gli utenti) di accedervi. Le risorse non locali possono così essere utilizzate dalle applicazioni, promuovendo l'efficienza e riducendo i costi [12].

Diverse amministrazioni

Ogni organizzazione può stabilire differenti politiche di sicurezza e amministrative che regolano l'accesso e l'utilizzo delle loro risorse. Di conseguenza, il problema della sicurezza della rete, di per sè già impegnativo, è ancor di più complicato dalla necessità di tener conto di molte condizioni.

Coordinamento delle risorse

Le risorse in un servizio di Grid devono essere coordinate al fine di fornire capacità di calcolo.

Accesso trasparente

Un servizio di Grid dovrebbe essere visto come un unico dispositivo virtuale [13].

Accesso affidabile

Un servizio di Grid Computing deve assicurare l'utilizzo dei servizi secondo alcuni requisiti riguardanti la qualità del servizio stesso. La necessità di un servizio affidabile è fondamentale dal momento che gli utenti, che richiedono garanzie sui servizi, riceveranno alti livelli di prestazione [14, 15].

Accesso costante

Un servizio di Grid deve essere creato secondo protocolli standard nascondendo così l'eterogeneità delle risorse e consentendo la scalabilità. Senza questi standard, lo sviluppo di applicazioni non sarebbe possibile.

Accesso persuasivo

Un servizio di Grid deve poter concedere l'accesso alle risorse disponibili adattandosi ad un ambiente dinamico. Ciò non implica il fatto che le risorse devono essere ovunque disponibili, ma che lo stesso servizio di Grid deve adattarsi, cioè deve trarne il massimo delle prestazioni dalle risorse disponibili [16].

1.5.2 Differenze tra Grid e Cloud Computing

La prima vera differenza è quella riguardante lo "job scheduling". Lo job scheduling è il vero scopo della tecnologia Grid, ossia quello di utilizzare tutti i tipi di risorse . Si può dividere un grande carico di lavoro in molti indipendenti job , e poi assegnarlo ad un nodo del Grid Computing. Anche se un nodo crasha, non importa , l'intero processo non sarà influenzato e lo stesso job sarà riassegnato ad altri nodi . Nel Cloud Computing le cose funzionano al contrario, in un certo senso, ovvero un singolo provider fornisce a più organizzazioni le risorse per l'esecuzione di applicazioni simili.
Un altro aspetto importante è la gestione delle risorse. Mentre il Grid si basa su sistemi batch, l'utilizzo delle tecnologie di virtualizzazione rappresenta la soluzione per il Cloud.
Un'altra differenza riguarda i modelli di erogazione di servizi. I modelli di erogazione del Grid sono basati su organizzazioni virtuali in cui i rapporti sono stabiliti offline. Nel Cloud l'utilizzo di SLA[8] e la gestione della fiducia è essenziale.
Un ultimo aspetto riguarda la disponibilità delle risorse. Nel Grid la condivisione di risorse si basa sul miglior sforzo possibile, ossia può accadere a volte che le risorse non siano disponibili e, talvolta, ci sono un sacco di risorse inattive. Nel Cloud le risorse sono disponibili in qualsiasi momento.

[8] SLA sta per Service Level Agreement e sono dei contratti stipulati tra un provider di servizi e il proprio cliente/i.

Capitolo 2: Service Level Agreement

2.1 LA virtualizzzazione delle risorse basata su SLA(SRV)

Un SLA (Service Level Agreement) è un contratto stipulato tra un provider di servizi ed il suo cliente; il cliente può essere una persona, un'organizzazione oppure un servizio. Il Cloud Computing rappresenta una recente infrastruttura di ricerca che si basa sugli ultimi risultati di diverse aeree di ricerca, come il Grid Computing, Service-Oriented Computing[9], processi aziendali e la virtualizzazione. Qui ci focalizzeremo su un'architettura per la virtualizzazione delle risorse basato su SLA che fornisce una soluzione per l'esecuzione di applicazioni utente nel Cloud. Questo lavoro rappresenta il primo tentativo di combinare le negoziazioni di risorse basate su SLA con risorse virtualizzate in termini di fornitura di servizi on-demand. La descrizione di tale architettura si basa su tre temi: contratto di negoziazione, brokering e implementazione del servizio utilizzando la virtualizzazione. Il Grid Computing [17] è riuscito a fornire servizi Grid per numerose comunità di utenti in tutto il mondo. Le tecnologie Web emergenti hanno già influenzato lo sviluppo del Grid; le più recenti soluzioni di molti campi di ricerca (ad esempio il P2P, ecc) devono anche essere prese in considerazione per trasformare con successo i Grid e i Service oriented Architectures (SOA) in servizi Internet [18]. Il Cloud Computing [19] è un candidato che mira alla creazione di questa sinergia; quindi viene presa in considerazione un'architettura Cloud concentrandosi sul contratto di negoziazione, brokering e implementazione del servizio utilizzando tecniche avanzate di virtualizzazione. Sia i servizi Grid sia le Service Based Applications(SBA) offrono già soluzioni per l'esecuzione di operazioni complesse. Il modello di servizio del Web si basa su tre attori: un fornitore di servizi, un richiedente di servizi e un mediatore di servizi [20]. Soluzioni di questo modello utilizzano tecnologie ben consolidate e molto utilizzate [20] che consentono la collaborazione tra queste tre parti in

[9] Per Service-Oriented Computing si indica genera generalmente un paradigma di calcolo che supporta l'uso di servizi-web per garantire l'interoperabilità tra diversi sistemi così da consentire l'utilizzo delle singole applicazioni come componenti del processo di business e soddisfare le richeiste degli utenti in modo trasparente.

grado di soddisfare le richieste degli utenti. Le esigenze emergenti degli utenti e ricercatori fanno si di ampliare questo modello di servizio con degli accordi e dei servizi di Grid ad alta intensità di calcolo. La maggior parte di alcuni lavori suddetti prendono in considerazione o gli approcci di virtualizzazione [21] [22] [23] senza prendersi cura della gestione dei Service Level Agreement (SLAs) o si concentrano solo sulla gestione degli SLA trascurando la virtualizzazione delle risorse [24] [25].
Di seguito viene presentata un'architettura basata su tre elementi principali: il contratto di negoziazione, il brokering e l'implementazione del servizio utilizzando la virtualizzazione. Elenchiamo gli attori della suddetta architettura:

- L'utente che vuole usare il servizio.

- MN - Meta-Negoziatore: una persona che gestisce i vari Service Level Agreement. Fa da mediatore tra l'utente e il Meta-Broker, seleziona i protocolli appropriati per gli accordi; gestisce la realizzazione e la violazione degli SLA.

- MB - Meta-Broker: il suo ruolo è quello di selezionare un broker (mediatore) che è in grado di implementare un servizio secondo le esigenze degli utenti.

- B - Broker: interagisce con le risorse virtuali e fisiche, e nel caso in cui il servizio richiesto deve essere implementato, il broker interagisce direttamente con la ASD.

- ASD – Automatic Service Deployment[10]: installa il servizio sulla risorsa selezionata on demand.

- S - Servizio: il servizio che gli utenti vogliono implementare o eseguire.

- R - Risorsa: macchine fisiche, sulle quali si possono implementare o installare le macchine virtuali.

[10] Sta per Servizio di Distribuzione Automatica.

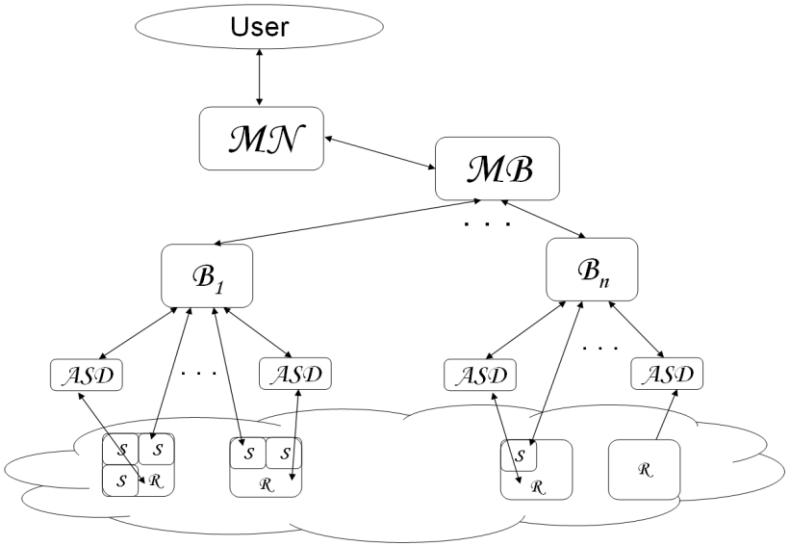

Figura 2 - Architettura SRV [27]

Gli attori dell'architettura interagiscono secondo i passi illustrati nella Figura 3:

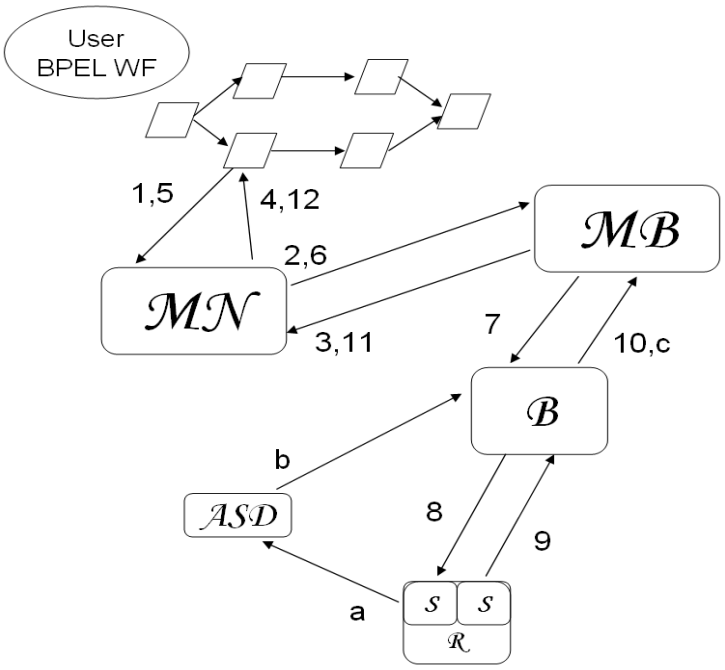

Figura 3 - Descrizione dei passi durante l'utulizzo del SRV [27]

- L'utente inizia una negoziazione per eseguire un servizio con determinati requisiti QoS[11], specificati in un SD (Service Description) insieme con il SLA (passo 1).

- MN chiede a MB se può eseguire il servizio secondo alcuni requisiti (passo 2).

[11] Qos (dall'inglese *Qualità di Servizio*) viene usato per indicare i parametri usati per caratterizzare la qualità del servizio offerto dalla rete, o gli strumenti o tecniche per ottenere una qualità di servizio desiderata.

- MB vede se i requisiti fanno match con le proprietà dei broker e risponde positivamente oppure con una differente offerta di “rinegoziazione”.

- MN risponde a MB. I passi 1-4 continuano finchè entrambe le parti abbiano trovato un accordo (per sottoscrivere un SLA).

- L’utente richiede il servizio secondo un certo SD e SLA (passo 5).

- MN passa all’MB la SD e il SLA eventualmente modificato (passo 6).

- MB chiama il Broker selezionato con il SLA e l’SD, eventualmente tradotto nella lingua del Broker (punto 7).

- Il Broker esegue il servizio secondo i termini del SLA (passo 8).

- I passi dal 9 al 12 rappresentano il risultato dell'esecuzione dal Broker, al MB, al MN ed infine all'utente.

- ASD monitora gli stati delle risorse virtuali e dei servizi implementati (passo a).

- ASD riporta la disponibilità e le proprietà del servizio al suo Broker (fase b).

- Tutti i Broker riportano le proprietà dei servizi disponibili al MB (passo c).

L'architettura precedentemente presentata e la procedura dettagliata di utilizzo mostrano che un accordo di negoziazione, il brokering e l’implementazione del servizio sono strettamente correlate e ognuno di essi richiede delle funzionalità per interagire senza problemi.

2.2 Requisiti e soluzioni per realizzare un SRV

In questo paragrafo vengono descritti le tre categorie principali di un sistema SRV, in cui sussistono i requisiti di base del sistema, sottolineando anche le interazioni tra queste componenti al fine di costruire un sistema conforme. In questo approccio proposto, gli utenti descrivono i requisiti per un SLA utilizzando il concetto di meta-negoziazione. Durante la meta-negoziazione vengono selezionati solo quei servizi di uno specifico linguaggio del documento SLA e che forniscono un'infrastruttura di sicurezza specifica. Dopo il processo di meta-negoziazione, una meta-broker seleziona un broker che è in grado di implementare un servizio secondo i requisiti dell'utente. Successivamente, il broker selezionato interagisce con le risorse virtuali o fisiche utilizzando il linguaggio richiesto dal documento SLA e la strategia di negoziazione specificata. Una volta che la negoziazione del documento SLA è conclusa, il servizio può essere implementato sulla risorsa selezionata utilizzando la virtualizzazione.

2.2.1 Accordo di negoziazione

Come mostrato in Figura 2 per realizzare un tale sistema occorre che le parti interagiscano in questo modo:

- Utente - MN: l'utente fornisce un documento di meta-negoziazione.

- MN - MB: decidono quali documenti di negoziazione usare, contenenti una specifica strategia di negoziazione, protocolli di negoziazione (WSLA, WSAg,), le condizioni di negoziazione (ad esempio il tempo, il prezzo) e l'infrastruttura di sicurezza.

- MB - B: decidono quale SLA usare, scritto in una lingua specifica (ad esempio WSLA, WS-Agreement) contenente dei parametri quali il tempo di esecuzione, prezzo, ecc.

- B - ASD: decidono quale servizio potrà essere disponibile sulle risorse gestite dall'ASD secondo alcuni vincoli di negoziazione; il servizio potrà utilizzare le risorse richieste senza interruzioni da altre parti.

- Inoltre, su ogni livello ci sarà bisogno (MN, MB, B, ASD) di un negoziatore che gestirà gli SLA.

Prima di impegnarsi a sottoscrivere un SLA, l'utente e il provider decidono quali parametri QoS adottare e le sanzioni nel caso uno di loro violi un SLA. Il termine strategia di negoziazione rappresenta la maniera in cui un socio decide quale fornitore o consumatore soddisfi le sue esigenze. Un protocollo di negoziazione rappresenta lo scambio di messaggi durante il processo di negoziazione. Recentemente, molti ricercatori hanno proposto diversi protocolli e strategie di negoziazione SLA nel Grid Computing [26]. D'altronde, essi non solo ritengono che le parti di una negoziazione assumano lo stesso protocollo, ma anche che condividano una visione comune circa i servizi in fase di negoziazione. In realtà però, un socio può preferire negoziare secondo determinati protocolli per i quali ha sviluppato strategie migliori, rispetto ad altri.

Per colmare il gap che esiste tra i diversi protocolli di negoziazione, di seguito viene proposta la cosiddetta architettura di meta-negoziazione [27]. In un documento di meta-negoziazione le parti partecipanti possono stabilire: i requisiti da soddisfare, per esempio, un metodo di autenticazione specifico o alcuni termini che vogliono negoziare (ad esempio il tempo, il prezzo, affidabilità); i protocolli di negoziazione e le lingue; le condizioni necessarie per stabilire l'accordo come ,ad esempio, viene messo in trattativa anche una terza parte. Questi documenti sono pubblicati in un registro consultabile attraverso cui le parti partecipanti potranno scegliere soci adeguati per lo svolgimento dei negoziati.

Le parti partecipanti seguono una struttura ben precisa del documento. La struttura del documento è costituita dalle seguenti sezioni principali: ogni documento è racchiuso tra i tag </meta-negotation>; ogni documento contiene un elemento <entity> che definisce le informazioni personali del partecipante, l'organizzazione a cui egli appartiene e un suo ID univoco.

```
1. <meta-negotiation ...>
2.   ...
3.  <pre-requisite>
4.   <security>
5.    <authentication value="GSI" location="uri"/>
6.   </security>
7.   <negotiation-terms>
8.    <negotiation-term name="beginTime"/>
9.    <negotiation-term name="endTime"/>
10.    ...
11.  </negotiation-terms>
12. </pre-requisite>
13. <negotiation>
14.  <document name="WSLA" value="uri" .../>
15.  <protocol name="alternateOffers"
16.    schema="uri" location="uri" .../>
17. </negotiation>
18. <agreement>
19.  <confirmation name="arbitrationService" value="uri"/>
20. </agreement>
21.</meta-negotiation>
```

Figura 4 - Esempio di un documento di meta-negoziazione [27]

Ogni documento di meta-negoziazione si compone di tre parti: i prerequisiti, la negoziazione e l'accordo (agreement), come mostrato in Figura 4. I prerequisiti definiscono il ruolo che un partecipante prende in un negoziato, le credenziali di sicurezza e i termini di negoziazione. Ad esempio, il tag sicurezza (</security>) specifica i meccanismi di autenticazione e autorizzazione che un partecipante vuole applicare prima di avviare la negoziazione, come per esempio, un cliente richiede che l'altra parte si deve autenticare tramite una GSI[12] [28]. I termini di negoziazione specificano gli attributi QoS che un partecipante è disposto a negoziare e sono specificati nell'elemento <negotiation-term>. Come mostrato in Figura 4, i termini di negoziazione del cliente sono il tempo di inizio e fine ed il prezzo. I dettagli sulla negoziazione sono definiti all'interno del tag <negotiation>. Ogni lingua del documento è specificata all'interno del tag <documento>. Una volta che la negoziazione si è conclusa e se entrambe le parti sono d'accordo riguardo i termini stabiliti, allora devono firmare l'accordo. Questo accordo può essere verificato anche da terze parti.

[12] Grid Security Infrastructure

2.2.2 Servizio di brokering

In questo paragrafo l'attenzione verrà focalizzata sugli aspetti del brokering relativi all'architettura SRV. I broker sono quei componenti a cui spetta il compito di trovare i servizi necessari con l'aiuto dell'ASD. Questo compito richiede diverse attività, come l'interazione con i sistemi informativi e depositi.

I broker hanno bisogno di interagire con l'ASD. Al livello superiore vi è anche un altro componente responsabile del brokering: il Meta-Broker (MB) [29]. Per Metabrokering s'intende la gestione delle risorse al livello superiore che utilizza risorse esistenti per poter accedere ad altre risorse. In modo più generale, il Meta-Broker funge da mediatore tra gli utenti e i gestori di risorse. I compiti principali di questo componente sono: raccogliere le informazioni del broker (i.e. la disponibilità, servizi implementabili, le risorse e le proprietà QoS relative all'esecuzione del servizio); interagire con il MN per stabilire degli accordi riguardo le chiamate di servizio, e di passare queste chiamate di servizio ai broker del livello più basso, per esempio confrontare le descrizioni dei servizi (SD) con le proprietà dei broker. Infine, la chiamata di servizio deve essere inoltrata al broker selezionato.

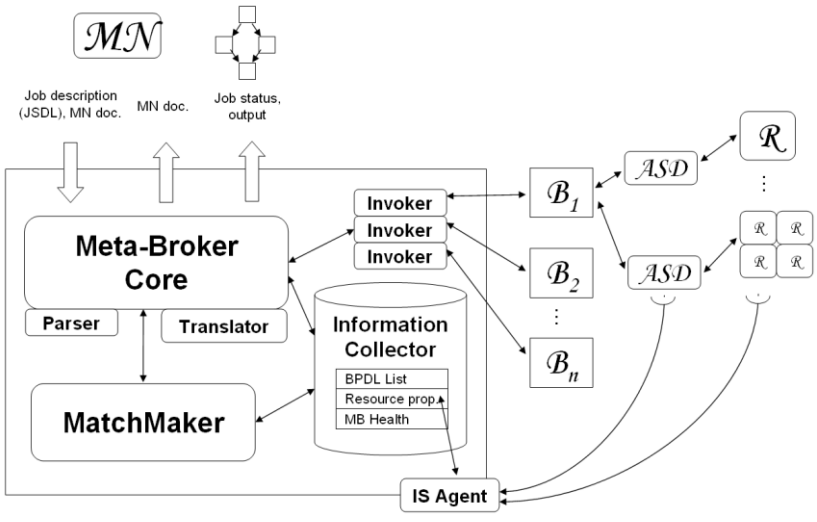

Figura 5 - Meta-Broker nell'architettura SRV [29]

La Figura 5 mostra come il Meta-Broker (MB) interagisce nell'architettura SRV e i componenti necessari per svolgere i compiti menzionati sopra. Molti broker utilizzano descrizioni di servizi (SD) diverse per comprendere le richieste dell'utente. Questi documenti devono essere scritti dagli utenti per specificare tutti i tipi di requisiti

relativi al servizio. In caso di utilizzo delle risorse nel Grid Computing, l'OGF[13] [30] ha sviluppato il cosiddetto JSDL[14], una specifica XML che descrive i job e i servizi di diversi broker e Grid, e in quest'ottica può esser vista la descrizione del Meta-Broker. Il componente *Translator* del Meta-Broker è responsabile della traduzione della specifica risorsa definita dall'utente nella lingua appropriata della risorsa del broker che il MB sceglie di utilizzare per una determinata chiamata. Questi broker possono soddisfare molte esigenze di utenti, quindi è necessario un linguaggio estensibile di markup per esprimere i metadata riguardo i broker e i loro servizi offerti, il BPDL (Broker Property Description Language)[31]. L'*Information Collector* (IC) memorizza i dati dei broker raggiungibili e delle precedenti richieste. Tutto questo mostra se il broker scelto è disponibile o quanto i suoi servizi siano affidabili. L'IC tiene traccia anche delle richieste andate a buon fine e non, in un documento BPDL. Per bilanciare il carico viene in gioco l'*agente IS* (IS sta per Information System), che supporta l'IC controllando regolarmente il carico delle risorse sottostanti di ogni broker, dopodiché memorizza i dati. L'IC comunica anche con gli ASD e riceve dati aggiornati riguardo i servizi disponibili. Il processo di matching delle richieste funziona così: il *MatchMaker* (MM) confronta le descrizioni delle richieste ricevute con il documento BDPL dei broker. Viene selezionato un gruppo di broker che soddisfi le suddette richieste e se non si trova questo gruppo di broker le richieste vengono rifiutate. L'IC tiene traccia di una lista di priorità dei broker e infine viene selezionato il primo broker della lista, poi il componente *Invoker* inoltra la richiesta al broker.

In conclusione, tre compiti principali spettano al MB: raccolta delle informazioni da parte dell'IS, gestione della negoziazione e selezione del servizio. Durante il processo di negoziazione il MB interagisce con il MN: esso riceve una richiesta con la descrizione del servizio (contenuta nel JSDL) e i termini SLA (contenuti nel documento MN) e va alla ricerca di un servizio raggiungibile da alcuni broker che rispettino i termini specificati. Se il servizio richiesto viene trovato, il documento SLA verrà accettato, altrimenti sarà rifiutato. Se i requisiti del servizio corrispondono a quelli dell'utente e, invece, i termini del SLA no, è possibile continuare la negoziazione modificando i suddetti termini e aspettare l'approvazione dell'utente.

[13] OGF sta per Open Grid Forum ed è una comunità di utenti, sviluppatori e venditori per la standardizzazione del Grid Computing.

[14] JSDL sta per Job Submission Description Language.

2.2.3 Virtualizzazione e implementazione del servizio

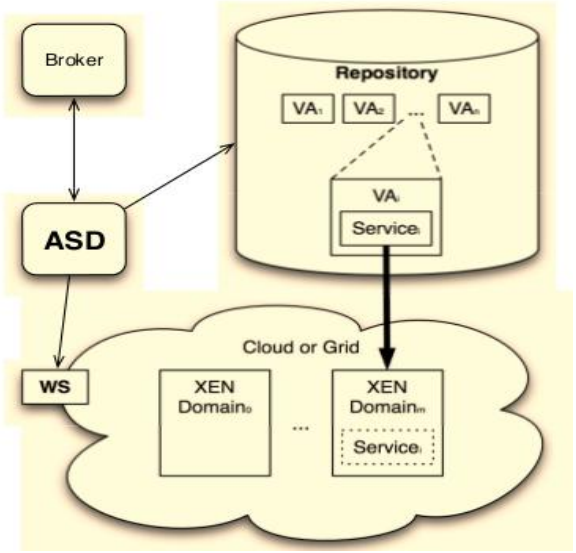

Figura 6 - Implementazione di un servizio nell'architettura SRV [33]

Nell'implementazione di un servizio entra in gioco l'ASD. La Figura 7 mostra i componenti di un ASD relativa all'architettura SRV. Per interagire con il broker l'ASD deve essere costruita su un repository. Tutte le copie originali di tutti i servizi implementabili devono essere immagazzinati nel repository. Allora la copia originale rappresenta tutto ciò che serve per implementare un servizio su un determinato sito, la quale copia viene chiamata applicazione virtuale (VA). La VA dovrebbe essere definita o da un'entità esterna oppure l'ASD dovrebbe acquisirla da un sistema già in esecuzione. Il repository permette al broker di sapere quali servizi sono disponibili per l' implementazione e quali sono quelli statici. In questo modo un repository sarebbe in grado di soddisfare una richiesta di un servizio prendendo in considerazione solo quei siti dove il servizio è stato implementato e dove potrebbe essere eseguito ma che non è ancora stato installato. Se i servizi implementati non sono disponibili, il repository controlla se qualche risorsa può fornire il servizio tenendo in considerazione il costo dell'implementazione. Il *Workspace Service* (WS) permette la creazione, la gestione e la rimozione di una macchina virtuale di un determinato sito come servizio WSRF[15]. Secondo l'OGSA, un tipico broker ha due legami col mondo esterno: il *Candidate Set Generators* (CSG) e i servizi di informazione. Il compito del CSG è di presentare una lista di siti che possono eseguire i servizi richiesti secondo il SLA e altri

[15] WSRF sta per Web Services Resource Framework ed è una famiglia di standard pubblicati da OASIS per servizi web.

requisiti; mentre i servizi di informazione offrono una panoramica generale sullo stato degli SBA (Service Based-Application), Grid e Cloud Computing. Nella maggior parte dei casi il CSG è parte integrante del broker il quale chiede una lista di siti come farebbe senza ASD. Il broker dopo aver valutato la lista, inizia l'implementazione di un servizio. La chiamata di servizio sarà eseguita come un servizio composto piuttosto che come una chiamata regolare. La composizione prevede l'implementazione come punto di partenza e la chiamata del servizio come compito dipendente. Poiché sia il CSG e i broker fanno affidamento sull'IS, l'ASD può influenzare la loro decisione attraverso la pubblicazione di dati. Questi dati potrebbero indicare la presenza del servizio su dei siti dove il servizio non è nemmeno implementabile. Il posto selezionato dall'ASD dipende dalle politiche del sito su cui si svolge il brokering. Nel caso le politiche del sito richiedano una restrizione particolare allora o il CSG o l'IS possono essere l'obiettivo prescelto. Se non vi sono restrizioni il broker in questione può essere sostituito dall'ASD. Nel caso in cui il CSG viene alterato allora fa una classificazione di risorse su cui la chiamata di servizio potrà essere eseguita [32]. Il CSG può fare la sua classificazione usando degli attributi specifici dell'IS locale. L'ASD opera con il CSG e il broker attraverso tre interfacce. Prima di tutto, i CSG formano una rete P2P la quale richiede due interfacce. La prima gestisce l'ontologia di diversi IS. La seconda supporta le decisioni prese tra i peer. La terza interfaccia giace tra il broker e il CSG e permette al broker di mandare un pacchetto riguardo la percentuale di successo dei siti candidati. I broker si devono adattare all'ASD, cioè se viene alterato il loro comportamento i broker possono prendere decisioni migliori. Dopo aver ricevuto l'insieme dei siti candidati, il broker fa una stima sui costi di implementazione di un dato servizio. Per la stima il borker interroga il WS. Se solamente viene alterato il comportamento del broker, e il CSG rimane intatto, allora l'ASD dovrebbe generare delle chiamate del servizio di implementazione sulle situazioni di sovraccarico (ad esempio, quando i requisiti SLA sono conclusi). Infine, è possibile modificare il comportamento dell'IS. In questo modo l'ASD fornisce delle informazioni sui siti, che possono accettare le chiamate di servizio dopo l'implementazione. L'ASD fa una stima sulle performance dell'IS (ad esempio il tempo di risposta stimato) e le pubblica. Queste stime riguardano coppie sito-servizio, e vengono pubblicate solamente quelle che superano una certa soglia. Per comunicare col broker l'ASD deve imporre dei vincoli riguardo il servizio richiesto indipendentemente da quale

macchina virtuale [33] venga usata. Per aiutare i broker a prendere delle decisioni riguardo quali siti usare l'ASD presenta dei costi di implementazione, contenuti negli SLA. L'ASD potrebbe iniziare l'implementazione o la disattivazione del servizio quando è in grado di evitare dei picchi riguardo l'uso del servizio e per far ciò deve essere a conoscenza degli accordi presi ai livelli superiori.

Capitolo 3: Sicurezza, Privacy e Accountability nel Cloud

3.1 Sicurezza

A parte i vantaggi che può offrire il Cloud Computing, come la flessibilità e i suoi bassi costi, vi sono molti problemi a riguardo e tutto ciò potrebbe avere un'influenza negativa sull'adozione del Cloud Computing in futuro come nuova infrastruttura IT.

Molti utenti condividono dati sensibili all'interno del Cloud. La mancanza di controllo nel Cloud è il problema principale. Una caratteristica per quanto concerne il controllo è la trasparenza nell'implementazione del Cloud. La trasparenza è necessaria per ragioni normative e per minimizzare il rischio di violazione dei dati. A causa della mancanza di controllo percepita ai tempi di oggi, le aziende più grandi stanno sondando il terreno con progetti più piccoli e dati meno sensibili. Il software open source consente ai dipartimenti IT di creare e distribuire applicazioni in modo rapido, ma a discapito di controllo e di governance.

L'integrità dell'infrastruttura del Cloud è garantita attraverso l'uso del Trusted Computing[16].

Il contenuto dei dati deve essere protetto in modo coerente secondo delle politiche, sia in azienda che nel Cloud. Ciò può esser ottenuto con la combinazione di server ad alta affidabilità e protocolli di crittografia che supportano il calcolo su testo cifrato. Tuttavia, poiché i meccanismi di protezione supportano il calcolo, è possibile per tutti gli utenti del Cloud beneficiare dei dati in modo controllato.

Ora vediamo dei problemi di sicurezza che impediscono alle aziende di trarre vantaggio dal Cloud. La Cloud Security Alliance[34] stila una tassonomia di domini di sicurezza che devono essere seguiti nell'implementazione del Cloud. Questi domini di sicurezza riguardano:

- Sicurezza tradizionale
- Disponibilità

[16] Per Trusted Computing (letteralmente "informatica fidata") si intende una nuova tecnologia in grado di rendere i dispositivi più sicuri mediante l'uso opportuno di software e hardware.

- Controllo dati da terze parti

Sicurezza tradizionale

Questi problemi riguardano i computer e le intrusioni della rete. I fornitori di Cloud rispondono a tali problemi dicendo che le loro misure di sicurezza sono più mature e collaudate rispetto a quelle delle medie-aziende. Un altro argomento, affrontato dal Forum Jericho [35] è:

"It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls."[17]

Tipici problemi di questa categoria sono: vulnerabilità dei Cloud provider, tentativi di phishing ai Cloud provider, autenticazione e autorizzazione.

Disponibilità

Questo tipo di problemi riguardano le applicazioni e i dati resi disponibili.

Problemi che appartengono a questa categoria sono quelli riguardanti l'uptime[18] dei server nei servizi Cloud; molti Cloud provider sostengono che l'uptime dei loro server regge bene con la disponibilità dei dati degli utenti. Infatti, come Leo Apotheker sostiene(11/24/08, searchSAP.com):

"There are certain things you cannot run in the cloud because the cloud would collapse."[19]

Altri problemi di questo tipo sono quelli riguardanti i Cloud provider che offrono maggior disponibilità ma più singoli punti di fallimento.

[17] "Potrebbe essere più semplice bloccare l'informazione da terze parti piuttosto che dall'interno, se le aziende sono preoccupate per le minacce interne…Inoltre, può essere più semplice far rispettare la sicurezza attraverso contratti con provider di servizi online piuttosto che attraverso i controlli interni."
[18] Per uptime si fa riferimento al tempo di attività funzionante di un apparato o sistema informatico.
[19] "Ci sono certe cose che non si possono eseguire nel Cloud perché il Cloud potrebbe collassare."

Controllo dati da terze parti

Le implicazioni legali di dati e applicazioni tenute da terze parti sono complesse e non ben comprensibili. Vi è anche una potenziale mancanza di controllo e trasparenza quando delle terze parti contengono i dati. Tuttavia, vi sono norme che richiedono trasparenza nel Cloud. Tutto questo sta spingendo alcune aziende a costruire Cloud privati per evitare questi problemi e mantenere alcuni dei vantaggi del Cloud Computing.

Un problema di questa categoria riguarda l'impegno dovuto dalle aziende, cioè se un utente può costringere un Cloud provider a rispondere entro un lasso di tempo stabilito. Un altro problema riguarda l'auditing[20]: l'auditing è un'altra conseguenza della mancanza di controllo; vi è sufficiente trasparenza nelle operazioni dei Cloud provider per scopi di auditing? Attualmente questa trasparenza è fornita dai manuali di auditing. Un altro problema riguarda le regole di governance del Cloud e i problemi contrattuali: riguardo questi ultimi, utilizzando un'infrastruttura di un'altra società, questa fa si che potrebbero esserci delle implicazioni giuridiche sorprendenti.

Un altro problema principale è la natura transitiva di alcuni Cloud, ossia che un provider di Cloud potrebbe aver stipulato contratti con altri, sui quali l'utente del Cloud ha ancor meno controllo. Un esempio è il servizio di archiviazione online chiamato The Linkup, che a sua volta utilizza una società di archiviazione online chiamata Nirvanix. Il fallimento di Linkup è dovuto all'aver perso quantità considerevoli di dati dei clienti, che alcuni dicono era colpa di Nirvanix [36]. Poiché l'adozione del Cloud Computing cresce, ci sono probabilità di vedere sempre più servizi che eseguono un mash-up dei dati. Questo crea potenziali problemi per la sicurezza, sia in termini di perdite di dati, sia in termini di numero di fonti di dati che un utente può avere. Un esempio è fornito da Facebook. Gli utenti di Facebook caricano sia i dati sensibili e non sensibili. Questi dati vengono utilizzati sia da Facebook sia da altre applicazioni. Queste applicazioni non sono tipicamente verificate da Facebook. Quindi, vengono create applicazioni maligne che girano nel Cloud di Facebook per rubare i dati sensibili [37]. L'ascesa del Cloud Computing ha creato set di dati che possono essere monetizzati da applicazioni come la pubblicità. Google, per esempio, sfrutta la sua infrastruttura Cloud per raccogliere e analizzare i dati dei clienti per la sua rete pubblicitaria.

[20] L'auditing consiste nella valutazione di un'organizzazione, sistema o processo. È mirato ad accertare la validità e l'affidabilità di un'informazione ed è anche una verifica del sistema di controllo interno.

La raccolta e l’analisi dei dati è ora possibile a buon mercato. Con il Cloud, gli aggressori hanno enormi banche dati centralizzate disponibili. A causa dei problemi di privacy, le imprese che eseguono le raccolta dei dati hanno sentito una pressione crescente nel rendere anonimi i loro dati.

3.2 Privacy

La privacy è un diritto umano fondamentale, sancito dalla Dichiarazione Universale delle Nazioni Unite dei Diritti Umani e dalla Convenzione Europea dei diritti dell'uomo. Ci sono varie forme di privacy[38]. Un tipo di privacy si concentra sui danni che derivano dalla violazione della privacy [39], e questo può fornire una base su cui sviluppare un'analisi dei rischi e benefici. I dati sensibili sulla privacy riguardano:

- Dati personali (PII): tutte le informazioni che potrebbero essere utilizzate per identificare o localizzare un individuo (ad esempio nome, indirizzo).
- Informazioni sensibili: informazioni sulla religione, salute, orientamento sessuale o altre informazioni che sono considerate private.
- Dati di utilizzo: i dati di utilizzo raccolti da dispositivi come stampanti, informazioni comportamentali quali abitudini di visione per i contenuti digitali, siti web visitati di recente dagli utenti.
- Identità di dispositivi: altri tipi di informazioni che potrebbero essere univocamente riconducibili ad un dispositivo, ad esempio, gli indirizzi IP.

Lo scopo degli ingegneri di software è quello di progettare servizi di Cloud in modo da diminuire il rischio di violazione della privacy. Leggi che mettono delle restrizioni geografiche ed altri tipi di restrizioni sui dati personali e sensibili limitano l’uso dei servizi Cloud. Ad esempio, un'azienda britannica, memorizzando i dati dei clienti con il fornitore di servizi di Cloud Salesforce.com, potrebbe trovarsi essa stessa in violazione della legge sulla protezione dei dati del Regno Unito; se il cliente del servizio è un’azienda, piuttosto che un utente, è più difficile dimostrare che un contratto, stipulato con un’azienda fornitrice di un servizio Cloud, sia ingiusto e sleale , perché le aziende sono meno protette rispetto

agli utenti, e Saleforce.com non dà ottime garanzie sulla sicurezza dei dati e non sarà responsabile nel caso di danni o perdita di questi ultimi[40]. I clienti possono citare in giudizio le aziende se i loro diritti sulla privacy venissero violati.

É anche importante rassicurare gli utenti circa l'utilizzo dei servizi Cloud. Agli utenti possono sorgere dei dubbi quando non è chiaro come le loro informazioni personali verranno utilizzate o trasmesse a terzi: questa mancanza di controllo porta al sospetto e, cosi, gli utenti diffidano del Cloud provider [41].

Gli aspetti chiave del Cloud Computing sono che ci sia un'infrastruttura condivisa tra le organizzazioni. Pertanto, ci sono dei rischi riguardo al fatto che i dati sono memorizzati e processati a distanza e c'è un crescente utilizzo della virtualizzazione tra utenti. La protezione dei dati personali e sensibili archiviati nel Cloud è quindi estremamente importante. I servizi possono essere aggregati e modificati dinamicamente da parte dei clienti, e i provider dei servizi possono cambiare il modo di fornire i servizi. In tal caso, i dati personali e sensibili possono esser scambiati all'interno di un'organizzazione, così da mantenere un'adeguata protezione delle informazioni e una conformità legale nonostante i cambiamenti.

La sicurezza dei dati nel Cloud è un problema chiave. I rapidi cambiamenti di ambienti Cloud sfidano le capacità delle imprese riguardo il mantenimento di standard di sicurezza coerenti. In particolare, il Cloud Computing consente ai nuovi servizi di essere disponibili mediante la combinazione con altri servizi: per esempio, un "servizio di stampa su richiesta" potrebbe essere fornito dalla combinazione di un servizio di stampa con un servizio di archiviazione. Questa procedura di combinazione di servizi è in genere meno controllata rispetto alle combinazioni di servizi precedenti svolte nell'ambito di sistemi aziendali multipartitici tradizionali. Ci potrebbero anche essere diversi livelli di controlli di sicurezza e privacy in ciascuno dei servizi componenti. D'altra parte, la fornitura di servizi potrebbe coinvolgere la raccolta, la memorizzazione e la divulgazione di informazioni personali e sensibili, e queste informazioni potrebbero aver bisogno di "spostarsi" attraverso i confini dei fornitori di servizi.

Inoltre, è molto probabile che sorgano nuovi rischi per la privacy visto che l'utilizzo del Cloud Computing aumenta: per esempio, i nuovi servizi che raccolgono e sfruttano i dati personali o finanziari.

3.2.1 Analisi di diversi tipi di contesto nel Cloud

Le minacce alla privacy variano in base al tipo di contesto nel Cloud. Alcune aree applicative e servizi del Cloud potrebbero trovarsi ad affrontare una bassissimo livello di minaccia per la privacy, per esempio, se il servizio elabora le informazioni che sono pubbliche. Solo quando il servizio gestisce le informazioni personali, cioè la raccolta, il trasferimento, l'elaborazione, la condivisione o la memorizzazione di esse, che ci potrebbe essere un rischio per la privacy e, in questo caso, la privacy deve essere presa in considerazione. Tuttavia, i servizi che vengono personalizzati dinamicamente , in base alla posizione delle persone, alle loro preferenze, al calendario e ai social network, richiederebbero che la privacy venisse presa in considerazione, in quanto il rischio è alto.
Analizziamo vari tipi di contesti:

Analisi sui dati di vendita. Un servizio di Cloud per l'archiviazione e l'analisi di un ampio database, per analizzare i dati di vendita, richiede una azienda commerciale (come Salesforce.com [42]). Un problema potrebbe essere il furto dei dati di vendita dal sistema del fornitore del servizio, e la sua possibile rivendita a concorrenti commerciali o ladri di identità.

Servizi su misura per l'utente finale[21]. Le informazioni possono essere raccolte automaticamente dall'utente finale e i suoi dati valutati, al fine di fornirgli servizi mirati secondo le proprie esigenze. Ad esempio, in uno contesto non commerciale, la gente può vedere quali dei loro amici siano vicini alla loro posizione attuale.

Le principali minacce in questi tipi di contesto coinvolgono:

- Le informazioni personali su un utente che vengono raccolte, usate, memorizzate e divulgate potrebbero non essere in conformità con i requisiti di questo utente.

[21] Per utente finale in questo contesto si fa riferimento al componente di un SLA sottoscritto tra il provider e l'utente stesso.

- Le persone che ottengono un accesso inadeguato o non autorizzato ai dati personali nel Cloud sfruttando alcune vulnerabilità, come la mancanza di procedimenti di controllo agli accessi, di buchi di sicurezza, i dati esposti “in chiaro”, politiche che sono modificabili da parte di soggetti non autorizzati, o copie di dati non protette e non controllati che vengono diffusi all'interno del Cloud.

- Nessuna conformità legale. In particolare, viene applicata la legislazione dei flussi transfrontalieri di dati, e anche alcuni dati possono essere visti come dati sensibili in senso giuridico, dipendente ciò dalla giurisdizione e dovrebbe essere applicata una legislazione più restrittiva a riguardo.

3.2.2 Rischi per la privacy nel Cloud

In sostanza, i principali rischi sono:

- *per l'utente del servizio di Cloud*: si può essere costretti o convinti di essere monitorati, dando informazioni personali contro la propria volontà.

- *per l'organizzazione utilizzando il servizio di Cloud:* nessuna conformità alla legislazione e alle politiche aziendali, perdita di reputazione e credibilità.

- *per gli implementatori di piattaforme Cloud*: l’esposizione di informazioni sensibili memorizzate su piattaforme (potenzialmente per scopi fraudolenti), responsabilità legale, perdita di reputazione e credibilità, la mancanza di fiducia degli utenti.

- *per i fornitori di applicazioni su piattaforme Cloud*: conformità non legale, perdita di reputazione.

- *per i soggetti interessati*: esposizione dei dati personali a occhi indiscreti.

Vi sono alcuni principi chiave per la privacy che minimizzano i rischi sopra citati tra cui [43,44,45]:

Avviso, lealtà e trasparenza: chi vuole usare le informazioni degli utenti deve dire loro quello che vogliono usare, come vogliono usarlo, per quanto tempo lo terranno, con chi lo condivideranno, e tutti gli altri usi che intendono fare con le informazioni. Essi devono anche informare gli utenti se vogliono fare un cambiamento riguardo al modo in cui viene utilizzata l'informazione. Se le informazioni devono essere trasmesse a terzi, questo deve anche essere comunicato. I dati personali devono essere raccolti direttamente dalla persona a meno che ci siano ottime ragioni per cui questo non sia possibile. Le politiche sulla privacy devono essere messe a disposizione dei clienti, ed essere comprensibili.

Scelta, autorizzazione e controllo: gli utenti devono avere la possibilità di scegliere se vogliono che le loro informazioni possano essere usate. Le persone interessate devono dare il loro consenso alla raccolta, all'utilizzo e alla divulgazione dei loro dati personali.

Necessità e minimizzazione: solo le informazioni che sono necessarie a soddisfare lo scopo prefisso devono essere raccolte e condivise. La raccolta dei dati dovrebbe essere minimizzata.

Accesso e accuratezza: gli utenti devono poter ottenere l'accesso alle informazioni personali, per vedere che cosa venga fatto e per verificarne la correttezza. Deve essere compiuto ogni sforzo per assicurare che le informazioni personali vengano tenute al sicuro.

Garanzie di sicurezza: le misure di sicurezza devono impedire l'accesso non autorizzato, la divulgazione, la copia, l'utilizzo o la modifica delle informazioni personali.

Scopo: l'utilizzo dei dati deve essere limitato allo scopo per cui sono stati raccolti. Ci deve essere un fine ben chiaro per la raccolta e condivisione delle informazioni personali. Gli interessati devono essere avvisati affinché i loro dati vengano raccolti e condivisi.

Limitare l'uso - divulgazione e conservazione: i dati possono essere solamente utilizzati o diffusi per lo scopo per cui sono stati raccolti e devono essere comunicati solo ai soggetti autorizzati a riceverli. I dati personali devono essere resi anonimi, ove possibile. I dati personali devono essere conservati per il tempo strettamente necessario.

Accountability: Un'organizzazione deve nominare qualcuno per assicurare che le norme sulla privacy vengano rispettate. Devono esservi presenti funzioni di audit per monitorare tutti gli accessi e le modifiche ai dati.

La legislazione è diversa a seconda del Paese in cui ci si trova. Tuttavia, i principi sopra citati si applicano alla maggior parte dei Paesi. C'è però una differenza: in Europa la privacy è un diritto fondamentale, mentre in Asia è basata di più sull'evitare i danni.
L'evoluzione del Cloud Computing può richiedere specifiche di progettazione particolari. In particolare, come i requisiti degli utenti, i requisiti di funzionalità possono cambiare così i requisiti di privacy devono essere riesaminati ad intervalli regolari. Inoltre, i modelli di governance dei dati devono tenere conto di tali infrastrutture che cambiano e ,di conseguenza, i requisiti di privacy possono variare significativamente nel tempo. I requisiti di progettazione sulla privacy variano per i diversi tipi di contesti. Ulteriori sforzi sarebbero necessari per sviluppare e valutare l'efficacia di nuovi modelli di progettazione della privacy su misura per i diversi tipi di contesto nel Cloud.

Accountability: una strada da seguire?

Nuovi modelli di governance per l'accountability possono anche costituire la base di un modo per affrontare i problemi di privacy nel Cloud Computing. Bisogna sottolineare comunque che l'accountability non sostituisce le leggi sulla protezione dei dati. Invece, la via da seguire per le organizzazioni è valutare l'accountability e quindi costruire meccanismi per una gestione dei dati più responsabile. In particolare, le organizzazioni

dovranno garantire che le norme che proteggono i dati (corrispondenti ai requisiti di legge) vengano rispettate da tutti coloro che fanno uso dei dati, indipendentemente da dove essi si trovino. L'accountability nel Cloud Computing potrebbe essere ottenuta tramite misure volte a collegare le politiche di sicurezza e privacy ai dati e a meccanismi per garantire che tali politiche vengano rispettate dalle parti che utilizzano, raccolgono e condividono i dati, indipendentemente dalla giurisdizione. Delle garanzie contrattuali vengono fornite all'organizzazione che vuole usare l'accountability da società che forniscono servizi di Cloud Computing , offrendo un adeguato livello di sicurezza e soddisfando le politiche fissate dall'organizzazione in questione, in particolare, la tutela dei dati personali.

3.3 Accountability

Per accountability si intende la capacità di un sistema di identificare un singolo utente, di determinare le sue azioni e il comportamento all'interno del sistema stesso [46]. L'accountability è un concetto che lega ciascuna attività al suo attore. Tale legame dovrebbe essere ottenuto facendo sì che tutti gli attori del sistema siano affidabili. Cioè, ogni attore potrebbe mentire sul proprio interesse. Quindi, questi legami devono essere supportati da prove dimostrabili o non contestabili. In linea di principio un sistema distribuito che fa uso di accountability è in grado di rilevare i guasti e ogni guasto può essere innegabilmente collegato ad almeno un componente difettoso o persona[47,48]. Un sistema che usa accountability deve avere le seguenti caratteristiche:

- **Identità:** Ciascuna azione (come l'invio di un messaggio) viene innegabilmente collegata al componente o alla persona che l'ha eseguita;

- **Registrazione sicura**: Il sistema deve tener traccia delle azioni passate in modo che gli utenti non possano falsificare o alterare le proprie azioni;

- **Auditing**: le registrazioni possono venir ispezionate in caso di anomalie;

- **Testimonianza**: Quando un auditor rileva un'anomalia, può ottenerne la causa che ha scaturito tale anomalia e può essere verificata in modo indipendente da terzi.

L'accountability sembra essere un approccio promettente per i problemi che abbiamo descritto sopra. I clienti di un servizio di Cloud Computing che fa uso di accountability potrebbero verificare se il servizio si stia comportando come concordato. Se si verifica un problema, il cliente e il fornitore potrebbero utilizzare le prove per decidere chi è il responsabile, e, qualora insorga una controversia, potrebbero presentare le prove a terzi, come ad esempio un giudice.

Tuttavia, le tecniche di accountability esistenti non soddisfano i requisiti per il Cloud Computing in diversi modi. Dal momento che il Cloud Computing è una piattaforma general-purpose[22], il provider dovrebbe essere in grado di offrire l'accountability per qualsiasi servizio.

È evidente che un servizio di Cloud Computing dovrebbe essere in grado di fornire l'accountability anche in presenza di un comportamento anomalo [49], cioè, anche se il cliente o il fornitore sono maligni, e anche se agiscono in collusione con alcuni o tutti gli utenti. A prima vista, questo requisito può sembrare troppo pessimista. Dopo tutto, le piattaforme Cloud attuali sono fornite da aziende del calibro di Amazon, Microsoft e Google, e queste aziende non commetterebbero intenzionalmente frode o agirebbero con cattiveria contro i loro clienti. È improbabile di solito che i fornitori di Cloud siano dannosi. Vi sono altre ragioni per cui alcuni fornitori o servizi siano definiti anomali. Un comportamento scorretto non è l'unica fonte di anomalie; gli attacchi di hacker, i bug di software, e le manipolazioni da parte di dipendenti scontenti o non soddisfatti possono causare effetti simili, e la loro individuazione non è meno importante di quella di un comportamento malevolo.

Infine, consideriamo il problema dal punto di vista del provider del servizio Cloud. Un comportamento dannoso da parte dei clienti è certamente una possibilità; ad esempio, i malintenzionati potrebbero tentare di estorcere denaro al provider minacciando di infangare la sua reputazione, o altri potrebbero cercare di incastrarlo facendo scaturire un sacco di

[22] Per general-purpose si indente un sistema o dispositivo che non sia dedicato ad un solo utilizzo, ma un sistema o dispositivo versatile che di solito carica componenti software che invece sono soluzioni specifiche ad una particolare esigenza

lamentele. Quindi, è probabile che la maggior parte dei fornitori rifiuterebbe di offrire l'accountability se ci fosse anche la minima possibilità che un servizio di Cloud, correttamente funzionante, potesse essere creato per apparire difettoso.

Quali sono gli incentivi del provider?

Dal punto di vista del cliente, ci sono evidenti vantaggi nell'utilizzare un servizio di Cloud Computing con accountability: il cliente può capire se il Cloud non esegue il servizio come concordato, e può considerare il provider del Cloud responsabile di questo. Dal punto di vista del provider del Cloud, d'altronde, l'accountability può apparire più come una potenziale fonte di problemi: può mettere il Cloud in cattiva luce, rivelando problemi che potrebbero invece non essere notati, e può fornire al cliente l'evidenza dei difetti. E allora perché un provider dovrebbe decidere di usare l'accountability?

Una ragione ovvia è che l'accountability sia allettante per i clienti. Tuttavia, ci sono anche benefici più diretti per il provider del servizio Cloud: egli può utilizzare l'accountability per rilevare e diagnosticare i problemi in modo intraprendente, e può facilmente gestire le lamentele dei clienti.

Attualmente è difficile per i clienti distinguere tra i problemi causati dal Cloud Computing e i problemi che essi stessi provocano; di conseguenza, i fornitori ricevono molte lamentele di cui non sono responsabili, questo senz'ombra di dubbio. Se vi è una tale lamentela, il cliente e il fornitore possono semplicemente eseguire una verifica per stabilire chi è responsabile.

La privacy può diventare un problema?

In alcuni contesti, c'è una tensione tra privacy e accountability, in quanto quest'ultima fornisce un resoconto dettagliato delle azioni di una macchina che poi può essere ispezionata da terze parti. D'altronde, è importante considerare ciò che si sta registrando, e a chi la registrazione viene resa disponibile. Un Cloud che fa uso di accountability potrebbe tenere i registri separati per ciascuno dei suoi clienti, e potrebbe rendere ogni registro

disponibile solo per il cliente che lo possiede. Quindi, il cliente A non dovrebbe capire nulla circa le azioni del cliente B (o anche che esistono altri clienti), e gli utenti non dovrebbero capire nulla circa le azioni di entrambi i clienti, perché non sarebbe stato permesso loro di controllare il Cloud a tutti gli effetti.

La domanda che rimane in sospeso è quella se l'accountability comprometterebbe la privacy del provider del Cloud nei confronti dei suoi clienti. A prima vista, la risposta potrebbe sembrare ovvia, dal momento che i clienti stanno pagando il provider del Cloud e quindi hanno tutto il diritto di sapere cosa viene fatto sul loro conto. Tuttavia, l'audit restituisce anche la prova dei guasti. Se la prova ha mostrato quale componente (router, firewall o server) del Cloud aveva causato il guasto, il cliente potrebbe fare inferenza sulla struttura interna del Cloud. D'altronde, questa informazione è ovviamente utile al fornitore, che è responsabile nel diagnosticare e risolvere il problema. Per ovviare a questo, il Cloud può tentare di fare delle prove in modo più dettagliato, a seconda di chi invoca l'audit.

L'accountability non può che rilevare e segnalare i guasti ma non mascherare i loro sintomi. Quindi, se si verifica un guasto nel Cloud, è possibile che il cliente o alcuni degli utenti ne risentano dei suoi effetti. Con la tecnica della tolleranza ai guasti, i sistemi possono continuare ad operare anche in presenza di guasti, cioè evitando i fallimenti. L'accountability integra le tecniche di tolleranza ai guasti rilevandoli ed isolandoli, impedendo loro di propagarsi al resto del sistema. Dato che non è possibile mascherare un guasto del tutto, le esecuzioni errate o sospette possono essere soppresse in modo che un tentativo di imbrogliare o rubare non sia possibile.

Naturalmente, ci si aspetta che la maggior parte dei fornitori di Cloud faranno del loro meglio per fornire un buon servizio, e per mascherare molti guasti. Tuttavia, è ancora utile far uso di accountability, in modo che il cliente possa verificare se il Cloud sia davvero affidabile come concordato, e il cliente e il fornitore siano in grado di rilevare e risolvere eventuali problemi che il Cloud non riesce a mascherare. Se l'accountability deve essere utilizzata, deve trovare un giusto equilibrio tra le esigenze del cliente e quelle del provider - cioè, deve evitare sia falsi negativi (per quanto concerne il timore da parte del cliente) che falsi positivi (il timore da parte del provider), e deve fornire loro le prove per risolvere eventuali controversie, possibilmente con l'aiuto di terzi. Per raggiungere quest'obiettivo, l'audit dovrebbe avere almeno le seguenti proprietà:

- **Completezza**: se viene violato l'accordo, l'audit riporterà eventualmente questo fatto, e fornirà la prova della violazione;

- **Accuratezza**: se l'accordo non viene violato, l'audit non segnalerà nessuna violazione;

- **Verificabilità**: qualsiasi prova di una presunta violazione può essere controllata in modo indipendente da un terzo, anche quest'ultimo non avrà fiducia né nel cliente né nel provider.

Queste garanzie si basano su poche assunzioni, ad esempio, non richiedono che i fornitori e i clienti si fidino l'un dell'altro, o che il Cloud sarà influenzato solo da guasti di un certo tipo. Avere garanzie solidi è certamente rassicurante, soprattutto in una tecnica come l'accountability che è destinata ad essere utilizzata quando le cose stanno andando male. È possibile rilasciare alcune di queste garanzie per ottenere diverse "sfumature" dell'accountability?

Non tutte le garanzie dell'accountability possono essere rilasciate tranquillamente. L'accountability viene vista come tecnica per far rispettare i contratti tra le imprese. Il rilevamento di un guasto può avere gravi conseguenze giuridiche e finanziarie per la parte responsabile. Quindi, la garanzia di accuratezza (elencata sopra) è assolutamente essenziale; una parte affidabile non deve essere biasimata per i guasti causati da altri, o per difetti che in realtà non si verificano. Tuttavia, questo problema non si applica necessariamente alle altre garanzie. Ad esempio, la completezza potrebbe essere resa probabilistica, cioè, il Cloud potrebbe rilevare ogni istanza di un guasto solo con un'alta probabilità.

Per implementare l'audit, abbiamo bisogno di conoscere le ultime azioni intraprese dalle varie entità del sistema (il cliente, il fornitore, gli utenti, le macchine del Cloud). In [47], prendendo come esempio un registro di anti-manomissione, possiamo vedere come ogni componente mantenga un registro in cui vengano riportati tutti gli input e gli output, compresi eventuali messaggi che invia o riceve, e permette ad altri componenti di valutare

questo registro. Il registro è strutturato in modo tale che gli auditor[23] possano rilevare se alcune voci sono state omesse, modificate o comunque manomesse. Se l'auditor rileva una presunta manomissione, ottiene anche la prova che può essere verificata in modo indipendente da un terzo.

I registri di anti-manomissione sono in grado di fornire una solida base per un servizio di Cloud che faccia uso di accountability. Se il cliente è in grado di controllare i registri delle macchine Cloud che sta utilizzando, può star certo di ottenere sia una corretta registrazione delle azioni passate di ogni macchina (il quale può controllare se vi è presenza di guasti) sia delle prove che alcune macchine non hanno mantenuto nei loro registri correttamente e sono, perciò, difettose. I registri di anti-manomissione offrono anche garanzie forti e dimostrabili, in particolare, è impossibile ottenere prove valide contro un componente o nodo corretto. Tale garanzia può aiutare ad allontanare alcune delle preoccupazioni del fornitore riguardo al fatto di essere accusato di colpe inesistenti.

Vediamo come un cliente riesca a riconoscere gli errori nei registri. Se il software è deterministico[24], si possono semplicemente riprodurre gli input del registro in un'istanza locale del software che il cliente ha installato nel Cloud, e confrontare gli output con gli output del registro. Transizioni di stato non corretti causano una discrepanza e possono quindi essere rilevati [47]. Tuttavia, non si può supporre che il software del cliente sia necessariamente deterministico, e non è sempre possibile apportare le modifiche necessarie per la registrazione e la riproduzione (ad esempio, se il codice sorgente non è disponibile). È possibile ottenere un effetto simile in un altro modo [50]: durante l'esecuzione originale, possiamo eseguire il software non modificato su una macchina virtuale, ed è possibile registrare tutti gli input o le prove non deterministiche, che si verificano sulla macchina virtuale. Durante un'operazione di audit, quindi, è possibile riprodurre questa esecuzione inizializzando un'altra macchina virtuale con la stessa immagine, e mettendo gli input registrati o le prove negli stessi punti durante l'esecuzione.

Alcune piattaforme Cloud esistenti come EC2 sono già basate sulle macchine virtuali, e non dovrebbe essere difficile aggiungere funzionalità come la registrazione e la riproduzione sulle loro macchine virtuali. Un problema maggiormente serio è che la riproduzione potrebbe richiedere la registrazione di una grande quantità di informazioni ed imporre un

[23] L'auditor è la persona che ha caratteristiche personali dimostrate e la competenza per effettuare un audit.
[24] Se è possibile prevedere l'output al 100%.

overhead[25] a run-time per la registrazione stessa. Comunque, i risultati di [50] indicano che questo overhead può essere abbastanza ragionevole. Un altro problema riguarda il costo di audit e di riproduzione.

La registrazione e la riproduzione possono essere utilizzate per rilevare le esecuzioni errate, ma questo è solo uno dei tanti problemi che un cliente di un servizo Cloud potrebbe essere interessato a rilevare.

Le violazioni degli SLA sono un altro grande problema; per rilevare queste violazioni, dobbiamo aggiungere delle informazioni sul tempo al registro di anti-manomissione. Ad esempio, è possibile poter includere periodicamente (ad esempio, una volta al secondo) nel registro un certificato di un servizio di timestamping di terze parti, come in [51]. Per ovvie ragioni, il servizio di timestamping non dovrebbe essere né controllato dal cliente né dal provider del servizio di Cloud.

Una volta che è stato possibile determinare i tempi dell'informazione nei registri, si può usarla per rilevare eventuali guasti. Tuttavia, se il fornitore è d'accordo per una specifica più dettagliata (ad esempio, in termini di latenza e velocità), dovrebbe essere possibile controllare più proprietà.

Se al cliente spettasse di rilevare i guasti ripetendo ogni singolo passo compiuto da una macchina Cloud, avrebbe bisogno di una secondo Cloud così da verificare l'andamento del primo, che sembra impraticabile per la maggior parte delle applicazioni. Un modo per ovviare a questo problema è di controllare più proprietà [52]. Un altro è quello di utilizzare il campionamento: possiamo ottenere una garanzia avendo un servizio di Cloud che esegue frequenti checkpoint, e permettendo al cliente di verificare a caso un piccolo numero di segmenti tra checkpoint consecutivi. Dal momento che molti problemi gravi (come ad esempio i guasti hardware) interesseranno molti o la maggior parte dei segmenti, il cliente può comunque rilevarli con un'alta probabilità, anche se la frequenza di campionamento è bassa.

Gli SLA spesso includono garanzie casuali, e a prima vista, il campionamento non sembra essere sufficiente per verificare queste garanzie. Ad esempio, se il fornitore promette che il 95% dei tempi di risposta sarà inferiore ai 100 ms, come può il cliente assicurarsi che non vi è alcun guasto senza controllare tutti i tempi di risposta? La risposta è che non si può, ma si

[25] L'overhead fa riferimento a delle risorse richieste in sovrappiù rispetto a quanto necessario per ottenere un determinato scopo.

può raggiungere arbitrariamente un'alta fiducia campionando un sottoinsieme ed eseguendo un test particolare[52]. Se il risultato è positivo, il cliente può confermare la presenza di un guasto scaricando e controllando un segmento del registro.

L'insieme delle tecniche che abbiamo visto fin qua, possono venir usate per avere un Cloud Computing che usi accountability. Tuttavia, non è ancora chiaro come realizzare l'accountability per altre proprietà, come ad esempio la riservatezza [53].

Un altro problema difficile è il supporto per i servizi dove gli utenti, che possono accedere alle macchine Cloud, non mantengono un registro di anti-manomissione. Tuttavia, sembra che la soluzione a questo problema per certe classi di applicazioni è fattibile. Ad esempio, i proxy potrebbero essere utilizzati per aggiungere l'accountability a un servizio web.

Chiaramente, un altro importante problema è la prestazione. Anche se ci sono prove che dimostrano che l'overhead è gestibile [50], c'è ancora da dimostrare che il costo di mantenimento, di trasferimento e di riproduzione dei registri di un servizio Cloud sia accettabile.

[54] contiene una panoramica dei problemi di sicurezza nel contesto dei servizi di Cloud storage, e cerca di affrontare tali questioni; [55] è uno studio più generale di Cloud Computing . Entrambi questi documenti sottolineano alcune questioni di cui abbiamo trattato finora. Precedentemente abbiamo mostrato come applicare l'accountability alle singole applicazioni [47, 56 , 57].

Il Trusted computing [58] è un approccio alternativo per raggiungere alcune delle garanzie che abbiamo elencato precedentemente. Tuttavia, esso richiede in genere grandi e complesse basi di codice, come l'hypervisor[26] o kernel, che sono ancora al di là della portata di tecniche di verifica all'avanguardia . Al contrario , alcune forme di accountability sono state attuate senza hardware speciale e con il codice molto poco attendibile . Altre forme (quali l'accountability per la riservatezza dei dati) possono richiedere un altro tipo di supporto.

[26] L'hypervisor è la componente più importante di un sistema basato su macchine virtuali

Capitolo 4: Conclusioni

Nella tesi è stato analizzato il Cloud Computing con tutti i suoi vantaggi e svantaggi, con le parti partecipanti che stabiliscono un contratto in modo da usare al meglio il servizio Cloud, chiamato Service Level Agreement (SLA) ed infine abbiamo analizzato la sicurezza e la privacy che vi sono dietro all'utilizzo del Cloud e l'accountability.

Abbiamo iniziato analizzando il Cloud Computing, definito come un nuovo approccio per l'erogazione di servizi IT. Uno dei più importanti vantaggi del Cloud Computing è che con esso non vi è più bisogno di investire in software, così abbiamo una diminuzione nei costi. Ci siamo soffermati sui tre modelli di servizio del Cloud: Iaas, Paas e Saas. Il Cloud viene suddiviso anche in Cloud pubblico, privato e ibrido. A volte bisogna fare distinzione tra Cloud e Grid Computing.

Nel secondo capitolo si è trattato degli SLA, accordi stipulati fra provider ed utente al fine di utilizzare al meglio il servizio. Abbiamo analizzato un'architettura basata sugli SLA (SRV) e caratterizzata da tre elementi principali: il contratto di negoziazione, il servizi odi brokering e l'implementazione del servizio utilizzando la virtualizzazione.

Infine abbiamo fatto un'analisi sulla sicurezza e la privacy che vi sono dietro l'utilizzo del Cloud Computing. Alcune imprese hanno sentito una forte pressione nel rendere anonimi i loro dati, quindi, abbiamo visto qual è l'impatto della privacy sui dati con tutti i suoi rischi e gli attacchi che vi possono essere. Può succedere che un utente del servizio potrebbe risultare colpevole a causa di un errore commesso da altre persone che utilizzano il servizio Cloud. Ed è qui che viene in gioco l'accountability. Quest'ultima fa in modo che le parti partecipanti usino il servizio in modo responsabile, assumendosi così le proprie responsabilità nel caso sorgano anomalie durante l'utilizzo del servizio. L'accountability integra anche le tecniche di fault tolerance, così da risalire a colui che ha generato il guasto nel sistema. L'accountability aumenta la fiducia degli utenti nell'utilizzare i servizi Cloud, che a prima vista possono sembrar rischiosi, garantendone una maggior diffusione.

Bibliografia

[1] Un nuovo approccio ad una vecchia tecnologia, http://aorakidesign.it/cloud-computing/

[2] Raccomandazioni e proposte sull'utilizzo del Cloud Computing nella Pubblica Amministrazione, http://www.agid.gov.it/sites/default/files/documenti_indirizzo/raccomandazioni_cloud_e_pa_-_2.0_0.pdf

[3] Virtualizzazione e Cloud Computing: i vantaggi, http://www.be1.it/virtualizzazione-e-cloud-computing-i-vantaggi/

[4] Cloud Computing Saas, Software as a Service http://www.hostingtalk.it/lezione-6-cloud-computing-saas-software-as-a-service_-c000000sI/

[5] Il bursting con HP CloudSystem, http://h20195.www2.hp.com/V2/GetPDF.aspx%2F4AA3-6847ITE.pdf

[6] I. Foster, C. Kesselmann, "The Grid: Blueprint for a New Computing Infrastructure", Morgan Kaufmann Publishers, USA, 1999.

[7] M.L. Bote-Lorenzo, Y.A. Dimitriadis and E. Gómez-Sánchez, "Grid Characteristics and Uses: A Grid Definition. Grid Computing". (Ed.). Springer Berlin / Heidelberg, pp. 291-298, 2004.

[8] I. Foster "The Grid: A New Infrastructure for 21st Century Science". Grid Computing. G. F. Fran Berman, Tony Hey (Ed.), pp. 51-63, 2003.

[9] I. Foster, C. Kesselman and S. Tuecke "The Anatomy of the Grid: Enabling Scalable Virtual Organizations". International Journal Supercomputer Applications, Vol. 15, No. 3, 2001.

[10] I. Foster, et al. “The Open Grid Services Architecture”, Version 1.0. Informational Document, 2005.

[11] I. Foster, “Globus Toolkit Version 4: Software for Service- Oriented Systems. FIP International Conference on Network and Parallel Computing”. Springer-Verlag LNCS 3779, pp. 2-13, 2005.

[12] Asensio, J.I., Dimitriadis, Y.A., Heredia, M., Mart´ınez, A., ´Alvarez, F.J., Blasco, M.T. and Osuna, C. From collaborative learning patterns to component-based CSCL application. In Proceeding ECSCW’03 workshop “From Good Practices to Patterns”, Helsinki, Finland, 2003.

[13] C. Crook, DeFanti, T., Foster, I., Papka, M., Stevens, R., Kuhfuss, T. “Overview of the I-WAY: Wide Area Visual Supercomputing”. International Journal Supercomputer Applications, Vol. 10, No. 2, pp.123–130, 1996.

[14] P. Dillenbourg, “Collaborative Learning: Cognitive and Computational Approaches”. Elsevier Science, Oxford, UK, 1999.

[15] I. Foster and C. Kesselman, “Globus: a Metacomputing Infrastructure Toolkit”. International Journal Supercomputer Applications, Vol. 11, No. 2, pp.115–128, 1997.

[16] M.L. Bote-Lorenzo, Y.A. Dimitriadis and E. Gómez-Sánchez, “Grid Characteristics and Uses: A Grid Definition. Grid Computing”. (Ed.). Springer Berlin / Heidelberg, pp. 291-298, 2004.

[17] C. Kesselman and I. Foster. The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann Publishers, November 1998.

[18] N. G. G. Report. Future for european grids: Grids and service oriented knowledge utilities – vision and research directions 2010 and beyond. Technical report, December 2006. ftp://ftp.cordis.lu/pub/ist/docs/grids/ngg3 eg final. pdf.

[19] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 2009.

[20] A. Tsalgatidou and T. Pilioura. An overview of standards and related technology in web services. Distrib. Parallel Databases, 12(2-3):135–162, 2002.

[21] K. Keahey, I. Foster, T. Freeman, and X. Zhang. Virtual workspaces: Achieving quality of service and quality of life in the grid. Sci. Program., 13(4):265–275, 2005.

[22] D. Reed, I. Pratt, P. Menage, S. Early, and N. Stratford. Xenoservers: Accountable execution of untrusted programs. In In Workshop on Hot Topics in Operating Systems, pages 136–141, 1999.

[23] I. Krsul, A. Ganguly, J. Zhang, J. A. B. Fortes, and R. J. Figueiredo. Vmplants: Providing and managing virtual machine execution environments for grid computing. In SC '04: Proceedings of the 2004 ACM/IEEE conference on Supercomputing, Washington, DC, USA, 2004. IEEE Computer Society.

[24] M. Surridge, S. Taylor, D. De Roure, and E. Zaluska. Experiences with gria – industrial applications on a web services grid. In E-SCIENCE '05: Proceedings of the First International Conference on e-Science and Grid Computing, pages 98–105, Washington, DC, USA, 2005. IEEE Computer Society.

[25] M. Q. Dang and J. Altmann. Resource allocation algorithm for light communication grid-based workflows within an sla context. Int. J. Parallel Emerg. Distrib. Syst., 24(1):31–48, 2009.

[26] M. Parkin, D. Kuo, J. Brooke, and A. MacCulloch. Challenges in eu grid contracts. In Proceedings of the 4th eChallenges Conference, pages 67–75, 2006.

[27] I. Brandic, D. Music, S. Dustdar, S. Venugopal, and R. Buyya. Advanced qos methods for grid workflows based on meta-negotiations and sla-mappings. In The 3rd Workshop on Workflows in Support of Large-Scale Science, pages 1–10, November 2008.

[28] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A security architecture for computational grids. In CCS '98: Proceedings of the 5th ACM conference on Computer and communications security, pages 83–92, New York, NY, USA, 1998. ACM.

[29] A. Kertesz and P. Kacsuk. Meta-broker for future generation grids: A new approach for a high-level interoperable resource management. In Grid Middleware and Services Challenges and Solutions, pages 53–63. Springer US, 2008.

[30] Open grid forum website. http://www.ogf.org, 1999.

[31] A. Kertesz, I. Rodero, and F. Guim. Data model for describing grid resource broker capabilities. In Grid Middleware and Services Challenges and Solutions, pages 39–52. Springer US, 2008.

[32] M. Taylor, C. Matuszek, B. Klimt, and M. Witbrock. Autonomous classification of knowledge into an ontology. In The 20th International FLAIRS Conference (FLAIRS), 2007.

[33] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles, pages 164–177, New York, NY, USA, 2003. ACM.

[34] Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.

[35] Don't cloud your vision. http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63-0000779fd18c.html?nclick_check=1.

[36] Loss of customer data spurs closure of online storage service 'The Linkup'. http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1.

[37] Facebook users suffer viral surge. http://news.bbc.co.uk/2/hi/technology/7918839.stm.

[38] The Royal Academy of Engineering, "Dilemmas of Privacy and Surveillance: Challenges of Technological Change", March 2007. Available via www.raeng.org.uk/policy/reports/default.htm

[39] D.J. Solove, "A Taxonomy of Privacy", University of Pennyslavania Law Review, vol 154, no 3, January 2006, p. 477. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622

[40] J. Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing", Computing, 24 Sept 2008. http://www.computing.co.uk/computing/features/2226701/clouded-uncertainty-4229153

[41] A. Tweney and S. Crane, "Trustguide2: An exploration of privacy preferences in an online world", Expanding the Knowledge Economy: Issues, Applications, Case Studies, P. Cunningham and M. Cunningham (eds), IOS Press, 2007.

[42] Salesforce.com, inc., Sales Force Automation web page, 2008. http://www.salesforce.com/products/sales-forceautomation/

[43] Organization for Economic Co-operation and Development (OECD), "Guidelines governing the protection of privacy and transborder flows of personal data", Paris, 1980 and "Guidelines for consumer protection for ecommerce", 1999. www.ftc.gov/opa/1999/9912/oecdguide.htm

[44] R. Clarke, "Xamax consultancy – PIA guidelines", 1999. http://www.xamax.com/au/.

[45] Information Commissioner's Office, "PIA handbook", 2007. http://www.ico.gov.uk/

[46] Accountability, http://it.wikipedia.org/wiki/Accountability

[47] Andreas Haeberlen, Petr Kuznetsov, and Peter Druschel. PeerReview: Practical accountability for distributed systems. In Proc. SOSP, October 2007.

[48] Aydan R. Yumerefendi and Jeffrey S. Chase. Trust but verify: Accountability for internet services. In ACM SIGOPS European Workshop, September 2004.

[49] Leslie Lamport, Robert Shostak, andMarshall Pease. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3):382–401, 1982.

[50] George W. Dunlap, Samuel T. King, Sukru Cinar, Murtaza Basrai, and Peter M. Chen. ReVirt: Enabling intrusion analysis through virtual-machine logging and replay. In Proc. OSDI, December 2002.

[51] Carlisle Adams, Pat Cain, Denis Pinkas, and Robert Zuccherato. RFC 3161: Internet X.509 public key infrastructure timestamp protocol (TSP). http://tools.ietf.org/rfc/rfc3161.txt, August 2001.

[52] Edmund M. Clarke, Orna Grumberg, and David E. Long. Model checking and abstraction. ACM Transactions on Programming Languages and Systems, 16(5):1512–1542, 1994.

[53] James Newsome and Dawn Xiaodong Song. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software. In Proc. NDSS, February 2005.

[54] Christian Cachin, Idit Keidar, and Alexander Shraer. Trusting the cloud. ACM SIGACT News, 40(2):81–86, June 2009.

[55] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical Report EECS-2009-28, University of California at Berkeley, February 2009.

[56] Nikolaos Michalakis, Robert Soul´e, and Robert Grimm. Ensuring content integrity for untrusted peer-to-peer content distribution networks. In Proc. NSDI, April 2007.

[57] Aydan R. Yumerefendi and Jeffrey S. Chase. Strong accountability for network storage. ACM Transactions on Storage, 3(3):11, 2007.

[58] Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues. Towards trusted cloud computing. In Proc. HotCloud, June 2009.

Ringraziamenti

Ringrazio Ilaria per avermi fatto compagnia durante questo periodo di studi.

Ringrazio la mia famiglia per avermi supportato durante il mio percorso di studi, dandomene la possibilità.

Ringrazio di cuore il gentilissimo prof. Fabio Panzieri per la sua disponibilità.

Ringrazio Massimo per avermi sostenuto in tutte le situazioni difficili e non e per i momenti passati insieme durante il periodo universitario.