Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Informatica

Meccanismi per l'attribuzione delle responsabilità nell'erogazione dei servizi di cloud computing: una rassegna

Tesi di Laurea in Reti di Calcolatori

Relatore:
Chiar.mo Prof.
Fabio Panzieri

Presentata da:
Luca Comellini

Sessione III
Anno Accademico 2010/2011

Indice

Introduzione

Lo scopo di questa tesi è quello di esaminare, discutere e valutare i meccanismi di accountability attualmente usati negli ambienti di cloud computing al fine di evidenziarne il ruolo nella diffusione di questi ultimi.

La mancanza di fiducia è riconosciuta come un ostacolo alla diffusione del modello *Software as a Service* (SaaS) del cloud computing; tuttavia le attuali condizioni contrattuali, oltre ad offrire poche assicurazioni, fanno ricadere i rischi sui consumatori. I potenziali utilizzatori di questo modello percepiscono di avere un minor controllo rispetto alle tradizionali architetture server e sono preoccupati per la loro privacy e l'integrità dei loro dati. Per di più, non è facile attribuire le colpe in eventuali casi di violazione della sicurezza o di perdita di dati.

Dal punto di vista legale la situazione non migliora: il flusso di dati tende infatti ad essere globale e risulta difficile stabilire dei confini geografici di competenza. Inoltre, aspetti come la virtualizzazione e l'auto-gestione possono apportare nuovi rischi, come il cross-VM (*Virtual Machine*), o una maggiore vulnerabilità dovuta alla mancanza di standard, alla "dynamic provisioning" o alla difficoltà di identificare la posizione fisica dei server.

Secondo l'*European Network and Information Security Agency* la perdita di "governance" è il principale rischio nel cloud computing, mentre la perdita di dati appare nella top 7 della Cloud Security Alliance (CSA) [1, 2].

L'accountability ci può aiutare ad affrontare queste nuove minacce, specialmente per proteggere le informazioni sensibili, per incrementare la fiducia degli utenti e per chiarire la situazione legale relativa al cloud computing.

Le innovazioni nella tecnologia hanno permesso di raccogliere e salvare dati in modi mai immaginati prima e le reti di telecomunicazioni si sono evolute per fornire un accesso ai dati continuo e a basso costo .

Il rapido aumento del flusso di informazioni, la loro raccolta, l'analisi ed il loro utilizzo, in aggiunta all'accesso globale, hanno creato una gamma di prodotti, servizi e risorse senza precedenti. Questi sviluppi però non hanno intaccato i già

presenti diritti inerenti alla protezione, alla sicurezza e ad un uso appropriato delle informazioni.

L'accountability non vuole ridefinire il concetto di privacy e sostituire leggi o norme già presenti, ma mira sostanzialmente a spostare l'attenzione sull'abilità di dimostrare che si è capaci di raggiungere determinati obiettivi riguardanti la privacy.

Il principio di accountability in riferimento alla protezione dei dati non risulta nuovo: ne troviamo infatti traccia per la prima volta nelle linee guida dell'OECD[1] e da allora ha avuto un ruolo sempre più importante nella gestione della privacy.

Il documento "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[2]" [3] è stato redatto principalmente per fronteggiare i numerosi problemi e pericoli sulla privacy e sulla libertà di utilizzo delle informazioni, collegati alla loro natura ed al contesto. Nel documento vengono illustrati i principi fondamentali che si dovrebbero applicare secondo l'organizzazione, tra cui il principio della qualità dei dati, dell'uso limitato, della salvaguardia della sicurezza e della trasparenza. L'*accountability* infine viene descritta come l'insieme di tutti questi principi.

Negli anni seguenti si sono susseguite diverse commissioni ed atti in riferimento a questo argomento; tra i più importanti troviamo il Canada's Personal Information Protection and Electronic Documents Act (2000) e l'Asia Pacific Economic Cooperation's (APEC) Privacy Framework (2005).

Anche all'interno dell'Unione Europea, quello dell'accountability diventa, nel corso degli anni, un concetto sempre più rilevante e fondamentale. Nonostante non fosse presente una chiara definizione nelle Direttive, numerose disposizioni richiesero alle organizzazioni di implementare processi di raccolta dati responsabili e sicuri. Nacquero anche numerose norme vincolanti relative al meccanismo per garantire una maggiore fiducia nella gestione dei dati personali delle imprese.

[1] OECD (*Organization for Economic Co-operation and Development*): organo internazionale con lo scopo di stimolare il progresso economico e il commercio nel mondo.
[2] Pubblicato dall'OECD nel 1980

Nel 2009 il progetto Galway[3] [4], formato da esperti e regolatori della privacy, diede la seguente definizione:

"Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information[4]".

I punti chiave sono quindi: la trasparenza, la responsabilità, la garanzia e l'obbligo di rimediare.

Il concetto dell'accountabilty verrà illustrato approfonditamente nel primo capitolo, soffermandoci sui suoi principali componenti, sulle sue funzioni e sui suoi sviluppi, mentre nella seconda parte della tesi analisi verrà analizzato il concetto del *cloud computing*.

L'idea che si trova alla base del meccanismo del cloud computing non è recente; infatti già nel 1960 John McCarthy aveva previsto che in futuro la computazione sarebbe stata offerta come un qualsiasi altro servizio, alla pari della corrente elettrica o del gas.

Il termine cloud deriva dal disegno di una *nuvola* usato dalle compagnie telefoniche per delimitare l'area di loro competenza. In seguito questa *nuvola* è stata usata per rappresentare Internet, come astrazione dall' infrastruttura sottostante.

Dopo che nel 2006 il CEO di Google, Eric Schmidt, usò la parola *cloud* nel descrivere un modello per fornire servizi attraverso Internet, questa definizione inizia a diventare sempre più popolare. Da allora è stato utilizzato non solo come termine negli ambienti di marketing, ma anche in contesti differenti per rappresentare idee diverse.

La mancanza di una definizione ufficiale ha creato molta confusione e scetticismo tra i potenziali utilizzatori e questo ha portato all'esigenza di trovare una definizione standard. Al fine di ottenere questo obiettivo sono stati di grande

[3] Iniziativa ideata dall'Ufficio Irlandese della Commissione per la protezione dei dati, co-sponsorizzata dall'OECD.

[4] "L'accountability è l'obbligo di agire come un amministratore responsabile delle informazioni personali altrui, di assumersi la responsabilità per la tutela e l'utilizzo appropriato di tali informazioni, al di là di requisiti di legge, e di essere responsabile per qualsiasi uso improprio di tali dati".

importanza i contributi di Vaquero, Merino, Caceres e Lindner (2009) [5] che hanno vagliato numerose definizioni provenienti dalle fonti più disparate, col fine di crearne una unica. Il denominatore comune tra tutte risultava essere la virtualizzazione, che rappresenta l'elemento chiave della tecnologia cloud e la base per ogni sua funzione.
La principale ragione di questa diversità di significati del cloud computing è che non si tratta di una nuova tecnologia, ma piuttosto di un nuovo modello che incorpora tecnologie già esistenti e consolidate, per offrire servizi in modo completamente nuovo, adattandosi alle richieste dell'attuale mercato.

Il *National Institute of Standards and Technology* (NIST) fornisce la seguente definizione: *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*[5]*"* [18].

Gli aspetti nuovi del cloud computing sono:

- L'illusione di infinita potenza di calcolo disponibile su richiesta e senza una pianificazione anticipata.
- Non è più necessario un grande investimento iniziale, permettendo così alle aziende di iniziare ad operare in modo graduale per poi ingrandirsi solo in base agli effettivi bisogni
- La possibilità di pagare l'utilizzo di risorse anche per brevi periodi in caso di necessità, per poi abbandonare il loro utilizzo quando non più necessarie.

Il cloud condivide alcuni aspetti con le seguenti tecnologie:

- *Grid computing*: un paradigma di computazione distribuita che coordina risorse in rete, anche lontane geograficamente.
- *Utility computing*: rappresenta un modello per fornire risorse on-demand, facendo pagare all'utente una tariffa legata al consumo piuttosto che fissa.

[5] "Il cloud computing è un modello che permette di abilitare in modo conveniente e on-demand l'accesso di rete a risorse di calcolo condivise (per esempio reti, server, storage, applicazioni e servizi) che possono essere rapidamente presi e rilasciati con il minimo sforzo di gestione o di interazione con il service provider.

- *Virtualizzazione*: si crea un livello di astrazione in cui non interessa il tipo di hardware sottostante e vengono fornite risorse virtualizzate per applicazioni di alto livello.
- *Autonomic computing*: termine coniato da IBM nel 2001, fa riferimento ad un sistema di computer capace di gestirsi autonomamente e di reagire a stimoli esterni ed interni senza l'intervento di un operatore.

Il cloud computing quindi sfrutta la virtualizzazione per fornire la computazione come utility, condivide alcuni aspetti del grid e dell'autonomic computing, ma differisce da questi per altri aspetti.

Il cloud computing può essere suddiviso in tre categorie in base al servizio offerto:

- *Infrastructure as a Service*: i clienti invece che comprare server, spazio in un data center o software, acquistano risorse on-demand generalmente tramite una Virtual Machine (VM). Alcuni esempi di *IaaS* provider sono Amazon EC2, GoGrid e Flexiscale.
- *Platform as a Service*: viene fornita una piattaforma completa, comprendente il sistema operativo e un ambiente di sviluppo, per facilitare l'implementazione di applicazioni senza doversi preoccupare dei costi e della complessità dell'acquisto e della gestione di tutti i livelli software e hardware sottostanti. Esempi di *PaaS* provider sono Google App Engine, Microsoft Azure, Force.com e Sun Cloud.
- *Software as a Service*: applicazioni on-demand tramite Internet. Esempi di *SaaS* sono Salesforce.com, Rackspace, Google Documents, DropBox.

Molto spesso i PaaS e SaaS provider fanno parte della stessa organizzazione ed è per questo che spesso si fa riferimento ad essi come *Cloud Provider*.

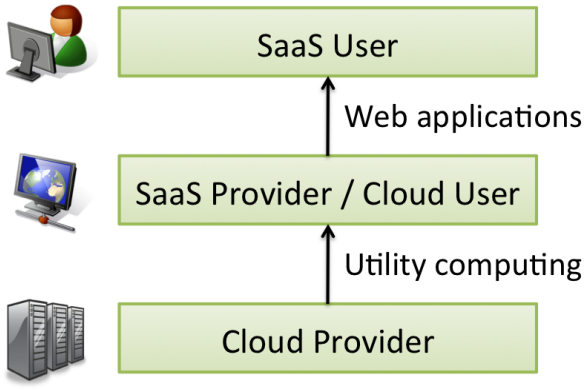

Figura 1: Utenti e Provider del Cloud Computing tratta da [7]

Ci sono vari aspetti da considerare quando si spostano delle applicazioni aziendali verso il cloud. Per esempio alcuni service provider vogliono soprattutto abbassare i costi mentre altri richiedono un servizio affidabile e sicuro.

Di conseguenza ci sono differenti tipi di cloud, ognuno con vantaggi e svantaggi:

- *Public cloud*: il service provider offre le risorse pubblicamente, tramite Internet. Questo tipo di cloud offre molti benefici al service provider, incluso l'annullamento di investimenti iniziali nelle infrastrutture e lo spostamento del rischio sui provider di quest'ultime. D'altra parte si ha la mancanza di un controllo capillare sui dati e sulle impostazioni di sicurezza o di rete.
- *Private cloud*: anche detto *internal cloud*, è progettato per l'uso esclusivo da parte di una singola azienda. Offre il massimo controllo sulla sicurezza, sull'affidabilità e sulle performance. La sua principale critica riguarda la similitudine alle tradizionali server farm, quindi senza i benefici tipici del cloud, come l'assenza di investimenti.
- *Hybrid cloud:* unisce i benefici del private e del public cloud e cerca di superare i limiti di questi due approcci. In un hybrid cloud si può per esempio avere una parte privata, con un maggior controllo dei dati più sensibili, ed una parte pubblica dove si dispone di risorse teoricamente illimitate. Questo approccio però richiede un attenta e ponderata pianificazione sulla divisione delle due parti.
- *Virtual Private Cloud* (VPC): soluzione alternativa per superare i limiti del private e del public cloud. Un VPC è essenzialmente un cloud pubblico

che sfrutta la tecnologia delle *Virtual Private Network* (VPN) per virtualizzare, oltre ai server e alle applicazioni, anche la rete sottostante. In questo modo i service provider possono gestire le loro regole di sicurezza e la topologia di rete [18].

Dopo aver fornito un quadro generale di questi due concetti, nella terza parte della tesi si tratterà l'accountability nell'ambiente cloud.
Inoltre, si è svolto un confronto tra i vari sistemi commerciali, tra cui Google AppEngine, Microsoft Azure e Amazon Elastic Compute Cloud.

Capitolo 1: Sicurezza e Accountability

1.1 Sicurezza Informatica

La *sicurezza informatica* è un ramo dell'informatica che si occupa dell'analisi del rischio, delle minacce, delle vulnerabilità di un sistema informatico e della protezione dei dati scambiati al suo interno. Questa protezione si può ottenere attraverso il monitoraggio degli accessi, permettendo solo quelli autorizzati (*autenticazione*), la fruizione dei soli servizi per cui l'utente è autorizzato, l'oscuramento (*cifratura*) delle informazioni scambiate tra gli utenti e la protezione del sistema da attacchi malevoli.

Negli ultimi tempi l'attenzione per la sicurezza informatica è aumentata per far fronte alla sempre più elevata informatizzazione della società e dei servizi, e per contrastare gli attacchi da parte di hacker specializzati, sempre più frequenti.

Si tende a suddividere la sicurezza informatica in due macroaree: *sicurezza passiva* e *sicurezza attiva*. La prima riguarda le tecniche e gli strumenti di tipo difensivo, che hanno l'obiettivo di impedire a utenti non autorizzati l'accesso a risorse, sistemi, impianti, informazioni e dati di natura riservata. Questo può includere anche l'accesso fisico ai locali dei server che vengono quindi protetti tramite l'utilizzo di porte blindate e di sistemi di identificazione personale, spesso anche biometrici.

Per *sicurezza attiva* si intendono invece le tecniche e gli strumenti mediante i quali le informazioni e i dati sono resi intrinsecamente sicuri, proteggendoli dall'accesso e dalla modifica da parte di utenti non autorizzati. I due tipi di sicurezza sono tra loro complementari ed entrambi indispensabili per raggiungere il livello di protezione necessario e desiderato all'interno di un sistema. Spesso chi

attacca un sistema informatico non è interessato al sistema in se, ma piuttosto ai dati in esso contenuti.

Le principali cause di perdita dei dati sono:

- *Eventi accidentali*: circostanze che non fanno riferimento all'attacco da parte di terzi, ma a eventi causati accidentalmente dall'utente. Ne sono alcuni esempi: l'uso sbagliato di un certo software o i guasti imprevisti magari dovuti a incompatibilità di componenti hardware.
- *Eventi indesiderati*: derivanti dalle azioni inaspettate da parte di terzi non autorizzati all'uso dei servizi o al trattamento dei dati. Fanno parte di questa categoria gli attacchi di hacker, utenti non autorizzati che si introducono nel sistema, riuscendo ad ottenere il pieno controllo della macchina, al fine di manipolarne il funzionamento e la disponibilità.

La sicurezza informatica comprende due attività distinte:

- *L'analisi del rischio:* consiste nella valutazione delle minacce, della loro probabilità di avvenimento e del danno stimato che potrebbero creare. A differenza del mondo fisico e materiale, le informazioni e le reti sono soggette sempre più a rischi di diversa natura, legati alla continua evoluzione. Risulta quindi rilevante effettuare questo tipo di analisi sostanzialmente per definire le minacce informatiche che si possono presentare, valutarne l'impatto e stabilire le contromisure per mitigare e ridurre i potenziali effetti. Permette quindi, in sintesi, di scegliere le soluzioni più corrette e coerenti per bilanciare i rischi e i costi. Il processo di analisi dei rischi è una componente fondamentale del Sistema di Gestione della Sicurezza, oltre ad essere richiesto da normative nazionali e comunitarie e da standard di riferimento come: l'ISF Standard of Good Practice, CobiT (*Control Objectives of IT Governance* dell' ISACA) ed il GMITS (*Guidelines for the Management of IT Security*). Un aspetto rilevante è la crescente importanza che l'analisi dei rischi informatici sta assumendo all'interno di contesti più ampi come l'analisi e la gestione dei rischi aziendali, (Corporate Governance) e di quelli finanziari (documento

di Basilea II[6]). Questo è dovuto al fatto che l'IT supporta sempre più il business ed i processi aziendali, influenzando e condizionando molte altre categorie di rischi (rischi operativi, finanziari o di mercato) [8].

- *La protezione dei dati:* si basa sui principi di disponibilità, integrità dei dati e riservatezza. Analizziamo più nel dettaglio quest'ultima attività.

1.2 La protezione dei dati

Ogni organizzazione deve essere in grado di garantire la protezione dei propri dati, in un ambiente dove i rischi informatici sono in continuo aumento.
Le imprese vedono a loro carico sempre più obblighi in materia di privacy, tra cui quello di compilare annualmente un documento specifico sulla sicurezza.
A livello internazionale è stato ideato il nuovo *Standard ISO 27001:2005*, finalizzato alla standardizzazione delle modalità di protezione dei dati e delle informazioni, per assicurarne l'integrità, la riservatezza e la disponibilità.
È una norma che illustra i requisiti stabiliti dal *Sistema di Gestione della Sicurezza delle tecnologie dell'informazione* (ISMS), ideata e pubblicata nel 2005 per fini certificativi. Il suo obiettivo è quello di definire un sistema completo per garantire la gestione della sicurezza, insieme alla sua linea guida (*ISO/IEC 17799:2005*), andando a sostituire la precedente norma di riferimento BS 7799 – ISMS.
I principali aspetti di protezione dei dati sono:

- la *confidenzialità* (o riservatezza), che riguarda la protezione dei dati e delle informazioni scambiate tra due soggetti, nei confronti di terze parti. Assume un'elevata importanza specialmente in sistemi di comunicazione intrinsecamente insicuri, come Internet. Vengono utilizzate tecniche di cifratura ed occultamento della comunicazione, che rendono il messaggio confidenziale. In un sistema che garantisce questo aspetto, le terze parti non hanno le capacità per decifrare il messaggio, reso illeggibile. Anche l'autenticazione permette di incrementare la confidenzialità, scartando gli accessi di soggetti non autorizzati.

[6] Documento che fa riferimento ad organismi bancari e finanziari, prevedendo un programma per la gestione dei rischi legati al business (come il rischio di credito o i rischi finanziari del mercato) e quelli operativi (come l'information risk).

- l'*integrità*, che consiste nella protezione dei dati e delle informazioni nei confronti di modifiche del contenuto, ad opera di terzi o per eventi accidentali. Questo aspetto garantisce anche la qualità del supporto che contiene i dati e del software. Insita nell'integrità è la possibilità di verificare con assoluta certezza se i dati siano rimasti inalterati nel loro contenuto durante lo scambio tra mittente e destinatario. La modifica ad opera di terze parti viene quindi rilevata.
- la *disponibilità*, cioè garantire l'accesso ai dati, alle informazioni e alle risorse nel sistema, da parte dei legittimi proprietari.

L'unione di queste tre aspetti è noto come il *Paradigma C.I.A.*, come mostrato dalla figura 2.

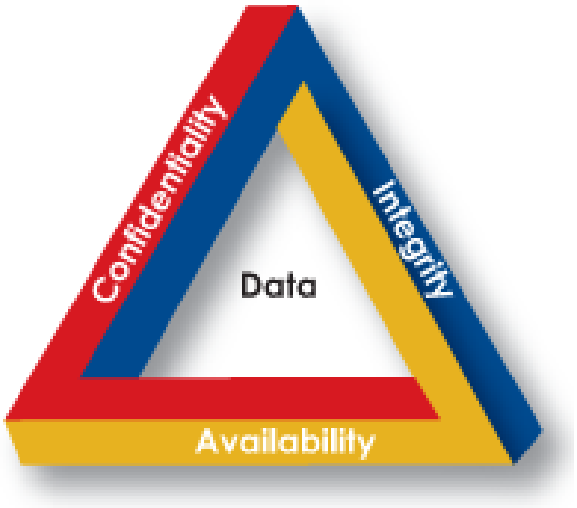

Figura 2: Il Paradigma C.I.A. [51]

Una completa protezione da attacchi informatici si ottiene agendo su più livelli: sia quello fisico e materiale, quindi connesso al luogo dove sono collocati i vari server, alla loro sorveglianza ed al controllo degli accessi, sia quello logico, che prevede l'autenticazione e l'autorizzazione dell'utente nel sistema.

Nel mondo informatico le minacce riscontrabili possono essere di tre tipologie:

- *Minaccia alla confidenzialità dei dati*: cioè la visualizzazione dei dati da parte di soggetti non autorizzati. La violazione può avvenire attraverso la mancanza del segreto d'ufficio, l'intercettazione del traffico di rete, una

cattiva progettazione dei controlli d'accesso, un sistema di autentificazione debole o infine per cola di virus o *spyware*[7].

- *Minaccia all'integrità dei dati*: si verifica quando utenti senza credenziali sono in grado di creare, modificare o cancellare dati ed informazioni. Le principali cause sono ascrivibili ad errori od omissioni nel sistema, virus maligni o attacchi informatici.
- *Minaccia alla disponibilità dei dati*: riguarda l'impossibilità di accedere al sistema da parte di chi ne ha i pieni diritti. Questo tipo di minaccia riguarda guasti o malfunzionamenti, attacchi di tipo DoS[8] o distruzione del sistema [9].

1.3 Diritto alla Privacy

Per *privacy* si intende il diritto di stabilire il livello di condivisione e di riservatezza dei propri dati personali. In altre parole "*the right to be let alone*"[9], secondo il documento "*The Right to Privacy*" di Samuel Warren e Louis D. Brandeis. Gli elementi sul quale si basa sono:

- *Anonimità*: la caratteristica che impedisce di raccogliere informazioni che potrebbero identificare una persona.
- *Riservatezza*: garanzia che i dati siano disponibili solamente ad utenti autorizzati.
- *Relatività*: la privacy non può essere assoluta, perché i rapporti e le interazioni sociali possono rivelare informazioni e dati personali.

Il valore della privacy risulta essere molto rilevante sia per l'individuo stesso, che ha il diritto di mantenere private e riservate le informazioni sulla propria persona, sui propri interessi e rapporti sociali, ma anche per una società fondata sulla libertà.

La privacy può essere protetta in due distinte modalità:

[7] Software che raccoglie informazioni sull'attività dell'utente, senza il suo consenso.
[8] *Denial of Service:* tradotto "negazione del servizio", sono attacchi eseguiti con l'obiettivo di rendere non disponibili alcune risorse o l'intero sistema.
[9] "*Il diritto di essere lasciati in pace*".

- *Strumenti tecnici*; riguardanti l'identificazione (negare l'accesso ad utenti senza credenziali), la cifratura (proteggere i contenuti) e l'anonimato (non rivelare l'identità dell'utente).
- *Strumenti legali*; composti da normative e leggi riguardanti la protezione della privacy.

Spesso però i problemi legati alla protezione della privacy vengono sottostimati dalle persone e dalle autorità, ad esempio perché sempre più servizi richiedono l'autenticazione, limitandone così il diritto stesso, oppure per via della limitata conoscenza degli strumenti di protezione della privacy o della leggi che aiutano a proteggerla.

Di crescente rilievo è il tema della protezione dei dati in riferimento a *Internet*, che è in grado di offrire un vasto numero di informazioni e di contenuti, ma allo stesso tempo può essere pericoloso per la privacy.

In un ambiente simile, garantire e mantenere l'anonimato può essere molto complesso: l'aumento costante del numero dei conti correnti online e la nascita di aziende esclusivamente sul web, ha fatto proliferare il numero di intrusioni non autorizzate.

Il mezzo forse più dannoso è lo *spyware,* software che istallandosi di nascosto sul computer dell'utente, invia dati personali (ad esempio pagine, siti visitati ed account) ad aziende che utilizzano le informazioni per rivenderle o per inviare una pubblicità più mirata. Gli *spyware* fanno parte di una più grande categoria di software, i *malware,* che hanno differenti funzioni: dall'invio di spam alla modifica della pagina iniziale o dei siti preferiti, ormai sino alla sempre meno frequente installazione di dialer che si connetto a numeri a tariffazione speciale.

Un'altra minaccia importante è rappresentata dall'ingegneria sociale (*social engineering*), una sorta di manipolazione psicologica che porta l'utente a compiere azioni o a divulgare informazioni riservate e si basa su specifici attribuiti del processo decisionale umano conosciuti come *distorsioni cognitive*. Quest'ultime vengono sfruttate in varie combinazioni per creare differenti tecniche di attacco, tra le quali troviamo: il *pretexting* (creare ed usare scenari inventati), il *baiting* (usare media fisici per incrementare la curiosità o l'avidità della vittima), il *phishing* (inviare e-mail indirizzando l'utente su siti falsi) o il *tailgating* (entrare in un'area protetta assieme a una persona autorizzata, fingendo di essersi dimenticati una chiave elettronica).

Il social engineering è tecnica molto complessa, visto che comporta un rapporto più diretto con la vittima dell'attacco, ma anche una delle più efficaci per carpire informazioni.

Alcuni accorgimenti da mettere in pratica per proteggersi da queste minacce sono:

- L'utilizzo di password lunghe, non banali e con codici alfanumerici;
- Evitare la comunicazione delle proprie credenziali via e-mail o tramite altri dispositivi;
- Installare, configurare ed aggiornare periodicamente antivirus e firewall;
- Controllare e monitorare i cookies;
- Non aprire allegati sospetti o proveniente da utenti sconosciuti;
- Utilizzare un efficace anti-spyware per controllare periodicamente il sistema;
- Leggere attentamente le licenze e le disposizioni sulla privacy prima di installare qualsiasi programma;
- Utilizzare la crittografia per messaggi privati.

1.4 Normativa Italiana sulla Privacy Informatica

La quantità di informazioni scambiate ed in possesso delle aziende è aumentata costantemente e la tutela dei seguenti dati ha fatto nascere numerose di controversie.

Nel nostro Paese, le leggi in riferimento alla privacy sono presenti nella Costituzione (articoli 15 e 21), nel Codice Penale (Capo III- Sezione IV) e nel *Testo unico sulla Privacy* (o codice della privacy).

Quest'ultimo documento è entrato in vigore il 1 gennaio 2004, approvato dal decreto legislativo n. 196 del 30 giugno 2003. In questo nuovo documento vengono introdotte le garanzie spettanti a tutti i cittadini, illustrate le semplificazioni e la razionalizzazione della cosiddetta "*legge madre sui dati sensibili*" (legge 675/1996[10]). Il codice mira quindi al riconoscimento del diritto del singolo sui propri dati personali, disciplinando le diverse operazioni di

[10] *"Legge per la Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali",* introdotta per rispettare ed applicare gli Accordi di Schengen ed entrata in vigore nel maggio del 1997.

gestione e di trattamento degli stessi, dalla raccolta all'elaborazione, dalla modifica alla cancellazione. Quindi scopo della legge è di evitare l'uso delle informazioni personali senza il consenso del soggetto interessato.

Il primo articolo del Testo Unico afferma che *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano",* facendo quindi riferimento ai diritti della personalità. L'articolo 3 invece afferma che:

"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità".

Il Testo è composto da tre parti:

1. *Disposizioni generali*, riguardanti le regole per l'uso dei dati personali, applicabili a tutti i trattamenti;
2. *Disposizioni particolari per specifici trattamenti;*
3. *Disposizioni relative alle azioni di tutela dell'interessato e al sistema di sanzioni.*

Il codice presenta quindi una sintesi degli obblighi e dei diritti per chi intende trattare o utilizzare dati ed informazioni personali. È necessario indicare con chiarezza le finalità dell'utilizzo e possedere il consenso del soggetto interessato.

Il Testo obbliga tutte le società, i liberi professionisti, enti o associazioni che trattano dati personali e sensibili, a redigere un *Documento programmatico sulla sicurezza* (DPS). Questo documento va predisposto ed aggiornato con scadenza annuale per attestare la corretta e coerente adozione ed applicazione delle procedure per il trattamento dei dati personali, adempiendo anche a determinati obblighi di legge.

Nel documento dovranno essere indicati:

- L'elenco dei trattamenti di dati personali;
- La distribuzione dei compiti e delle responsabilità nel trattamento dei dati;
- La descrizione dei criteri e delle modalità per il ripristino dei dati in seguito a danneggiamento o distruzione di essi;
- Analisi dei rischi sui dati;

- Eventuali previsioni per interventi formativi per gli incaricati al trattamento dei dati.

1.5 Accountability

L'*Accountability* è un concetto di etica e governance a cui vengono attribuiti diversi significati. Molte volte viene utilizzato come sinonimo di responsabilità, intesa come "rendere conto" [10].

Come aspetto di *governance* invece è stato rilevante nelle discussioni riguardanti il settore pubblico, quello no-profit e quello privato. In questi ambiti viene intesa come il riconoscimento e l'assunzione della responsabilità in riferimento alle azioni, ai prodotti, alle decisioni e alle politiche di un sistema o di un'organizzazione, ma significa anche essere responsabile per le possibili conseguenze derivanti da un cattivo uso di essa [11].

Una gestione dei dati secondo l'approccio dell'*accountability* si caratterizza per l'attenzione alla protezione della privacy ed una forte discrezionalità nel determinare misure per conseguire gli obiettivi prestabiliti, attraverso metodi e pratiche coerenti e responsabili.

Un approccio basato sulla responsabilità e sulla tutela dei dati sensibili offre vantaggi immediati alle persone, alle istituzioni ed alle autorità di regolamentazione [12]. In particolare:

- Aiuta il collegamento tra diversi sistemi normativi, consentendo ai paesi di perseguire obiettivi comuni di protezione dei dati. Questo favorisce lo scambio di informazioni, permettendo a queste di muoversi attraverso le frontiere, garantendo un livello comune di protezione e di sicurezza.
- Aumenta la fiducia delle persone in riferimento ai loro dati sensibili, riducendo le preoccupazioni legali.
- Aumenta la qualità della protezione delle informazioni, consentendo l'uso di strumenti che riducono rischi e che rispondono ai nuovi modelli di business e di tecnologie.
- Permette alle organizzazioni di avere una maggiore flessibilità ed un uso più efficace delle scarse risorse destinate alla protezione della privacy.

1.6 Accountability nell'informatica

Inizialmente il termine *accountability* veniva utilizzato nel settore informatico in riferimento ad un requisito, limitato ed impreciso, ottenuto tramite l'audit e le segnalazioni [6].

Ora questo contesto riguarda sostanzialmente la capacità di un sistema di determinare i comportamenti e le azioni al suo interno, creando e conoscendo l'identità di ogni singolo utente.

Trattandosi di un aspetto rilevante della più ampia attività del controllo degli accessi, si basa sul principio della responsabilità delle azioni degli individui all'interno del sistema. Quest'ultimo è responsabile se fornisce un mezzo per rilevare e denunciare comportamenti scorretti da parte dei suoi utenti.

Si parla di *responsabilità forte* se ad ogni soggetto viene fornito un mezzo per comprendere autonomamente se gli altri utenti si stanno comportando correttamente, senza fidarsi di affermazioni di altri utenti, che potrebbero essere compromessi. L'accountability quindi fornisce incentivi alla cooperazione e scoraggia comportamenti dannosi.

Risulta un aspetto fondamentale in molti framework relativi alla tutela della privacy, tra cui le linee guida stabilite dall'OCSE (1980), il Canada's Personal Information Protection and Electronic Documents Act (2000) e l'APEC[11]'s Privacy Framework (2005).

Inoltre, i modelli di governance di molti Paesi si stanno evolvendo per incorporare il principio di accountability ed un uso responsabile e corretto delle informazioni. Nello specifico, le autorità legislative stanno sviluppando framework, come il BCRSs[12] e l'APEC's Cross Border Privacy Rules, dove si fornisce un approccio unico e pratico alla protezione dei dati nei diversi sistemi regolatori. Nel primo documento, ad esempio, si obbligano le organizzazioni a dimostrare di essere conformi ai requisiti stabiliti dall'Autorità dell'Unione Europea per la protezione dei dati trasferiti fuori dall'EU [6].

L'*accountability* presenta degli elementi essenziali, che costituiscono condizioni necessarie per le organizzazioni che vogliono stabilire, dimostrare e testare la loro responsabilità. Componenti centrali sono la trasparenza, la responsabilità,

[11] Asia Pacific Economic Cooperation
[12] EU's Binding Corporate Rules.

l'assicurazione e la capacità di rimediare. Le organizzazioni devono dimostrare di aver riconosciuto ed assunto la responsabilità, sia in termini di politiche adeguate, sia in termini di buone pratiche, comprendendo la correzione e la capacità di rimediare in caso di errori o cattiva condotta. Queste organizzazioni devono adottare un processo decisionale responsabile, in particolare riferendo, spiegando e rispondendo per le conseguenze delle decisioni che hanno preso riguardo alla protezione dei dati.

In [12] le organizzazioni vengono misurate in base a:

- *L'impegno all'accountability e l'adozione di politiche interne coerenti con i criteri esterni*. L'organizzazione deve dimostrare la sua disponibilità e la sua capacità di essere responsabile nelle pratiche riguardanti i dati.
- L'organizzazione deve implementare politiche legate a criteri esterni come leggi, principi, e best practices del settore, progettarle attentamente per garantire un'efficace tutela della privacy, implementare i meccanismi necessari e monitorare quest'ultimi. Tali meccanismi e tali pratiche devono essere approvate dal più alto livello dell'organizzazione.
- *I meccanismi per attuare le politiche sulla privacy, compresi strumenti, formazione ed educazione*. L'organizzazione deve stabilire i procedimenti per l'attuazione delle politiche sulla privacy dichiarate e stabilite. Possono includere strumenti per facilitare il processo decisionale per un uso corretto dei dati ma anche la formazione e l'educazione sul loro utilizzo. Questi meccanismi sono obbligatori per le persone chiave coinvolte nella raccolta e nella diffusione delle informazioni personali.
- *Sistemi per la supervisione interna e la verifica esterna*. Le imprese devono monitorare e valutare se le politiche adottate siano applicate in modo efficace e se siano stabilite con l'obiettivo di proteggere i dati sensibili raccolti. L'organizzazione dovrebbe periodicamente impegnarsi nel verificare e dimostrare i propri requisiti di accountability. Tale verifica può comprendere anche valutazioni ad opera di terze parti.
- *Trasparenza e meccanismi di partecipazione individuale*. Per facilitare la partecipazione individuale, le procedure dell'organizzazione devono essere trasparenti. La strategia scelta, ma anche tutte le informazioni rilevanti, devono essere ben visibili e comunicate ad ogni individuo

interessato. Quest'ultimo dovrebbe essere in grado di conoscere i dati che vengono raccolti dall'organizzazione, bloccarne eventualmente la raccolta e l'utilizzo nei casi in cui non sia appropriato e correggerlo quando è impreciso.

- *Mezzi per la riparazione e l'applicazione esterna.* Quando sussistono danni alla privacy o dimenticanze nella sua conformità, l'individuo dovrebbe avere accesso ad un meccanismo di ricorso nei confronti dell'organizzazione. L'organizzazione dovrebbe prima di tutto identificare l'individuo colpito e fornire un primo contatto per la risoluzione delle controversie; successivamente dovrebbe stabilire un processo attraverso il quale i reclami vengono revisionati ed indirizzati. L'azione di terze parti può facilitare l'interazione tra il consumatore e l'organizzazione, migliorandone la reputazione ed il rispetto degli obblighi.

Molti sostengono che per fornire accountability sia necessario passare dal nascondere l'informazione all'assicurare che ne venga fatto solo un uso appropriato. L'utilizzo delle informazioni deve essere trasparente, in modo da poter determinare eventuali accessi non autorizzati o non conformi alle regole.
I cloud provider permettono di conservare e mantenere uno storico delle manipolazioni dei dati, che possono essere controllate e monitorate rispetto alle politiche che li governano. Questo definisce la cosiddetta *accountability retrospettiva:* se un attore A svolge l'azione B, allora si può esaminare quest'ultima azione rispetto ad una politica predeterminata per decidere se A si è comportato in modo scorretto e quindi ritenerlo responsabile.
Si deve estendere questo approccio includendo anche gli *effetti prospettivi* dell'accountability perché l'ambiente potrebbe mutare: per esempio potrebbero insorgere nuovi rischi per i soggetti legati ai dati, potrebbe avvenire un cambiamento di proprietà del cloud provider o potrebbe mutare la posizione fisica dei server.
Ridurre il rischio di un danno, riduce le conseguenze negative che i controllori delle informazioni potrebbero subire. Per farlo è necessario costruire e rafforzare nei processi delle best practices in modo che la responsabilità del danno non sorga.

Questo è un processo riflessivo della privacy che non risulta essere statico e nel quale i controllori delle informazioni devono effettuare una valutazione continua dei possibili danni ed un processo di revisione durante tutta la prestazione del servizio o del contratto.
In generale quindi, un approccio legato all'accountability richiede alle organizzazione di:

- Impegnarsi ad essere responsabili e stabilire politiche coerenti con i criteri esterni riconosciuti;
- Fornire trasparenza e meccanismi per la partecipazione individuale, compresa la condivisione delle politiche scelte con i propri stakeholders, sollecitando un loro feedback;
- Utilizzare metodi per attuare piani responsabili, tra cui una chiara comunicazione ed una corretta documentazione, supportate a tutti i livelli della struttura organizzativa;
- Fornire mezzi per l'applicazione esterna, il monitoraggio ed il controllo;
- Fornire meccanismi per correggere e rimediare ad eventuali danni o ad azioni scorrette. Deve includere la gestione dell'evento e la gestione dei reclami [6].

L'accountability viene supportata da altre due attività:

1. *Audit*, spesso usato per rilevare intrusioni o per eventi passati. Rappresenta una valutazione tecnica, manuale o automatica del sistema o di una qualsiasi applicazione informatica. Quella manuale consiste in domande eseguite allo staff, nell'esecuzione delle analisi di vulnerabilità, nella revisione e nel controllo degli accessi alle applicazioni, al sistema operativo e gli accessi fisici ai sistemi (server, computer, router, ecc). Le valutazioni automatiche invece includono rapporti generati dal sistema o dal software per controllare e riportare mutamenti a file o impostazioni del sistema.
2. *Login,* cioè la procedura di autenticazione in un sistema o ad una applicazione informatica. Tipicamente dopo aver inserito un nome utente e una password, il sistema controlla che la password corrisponda a quella presente in un elenco di autenti autorizzati e permette l'accesso secondo i

diritti di cui l'utente dispone. Una volta che l'utente è autenticato, si può tenere traccia delle operazioni che svolge e segnalare se cerca di compiere azioni per cui non è autorizzato.

Infine, fu la Baronessa O'Neill[13] a proporre per la prima volta il concetto di *intelligent accountability,* come mezzo per fornire una maggiore responsabilità senza però danneggiare le prestazioni professionali [13]. Sosteneva che la gran parte degli aspetti di cui gli individui e le organizzazioni devono dar conto non è facilmente misurabile e non possono essere ridotti ad un semplice set di indicatori della performance. Questo particolare tipo di responsabilità "*richiede maggiore attenzione per una buona governance e meno fantasie sul controllo totale*" e che "*una buona governance è possibile solo se le istituzioni sono autorizzate ad un marginale autogoverno in riferimento ai loro compiti particolari*".

È necessario introdurre *accountability* in modo intelligente nel sistema, altrimenti la fiducia non aumenterà e gli effetti complessivi potrebbero essere negativi, a causa degli ulteriori oneri amministrativi [6].

1.7 Esempi di Accountability

1.7.1 Archiviazione di rete

CATS[14], è un servizio di archiviazione di rete con una proprietà di *strong accountability*. Un server CATS annota le risposte lette e scritte, che rappresentano la prova di un corretta esecuzione e offre interfacce di controllo, consentendo ai clienti di verificare che il server sia affidabile. Un server guasto non può nascondere il suo cattivo comportamento, e le prove delle azioni scorrette sono verificabili in modo indipendente da qualsiasi partecipante. I client CATS sono anche loro responsabili per le azioni che compiono nel servizio. Un client non può negare le sue azioni ed il server può provare l'effetto che hanno avuto. I risultati di alcuni test mostrano che una *strong accountability* è pratica per i sistemi di archiviazione di rete in ambienti con una forte identità e con un basso grado di scritture condivise [14].

[13] Professoressa di filosofia all'Università di Cambridge e nel 2003 è stata la presidentessa fondatrice della British Association Philosophical (BPA)
[14] Acronimo di "Certified Accountable Tamper-evident Storage"

1.7.2 Database

I database che permettono di conservare record storici delle attività e dei dati, offrono numerosi benefici per l'accountability di un sistema: gli eventi passati possono essere analizzati per mantenere la qualità dei dati e per individuare le infrazioni. Allo stesso tempo la conservazione della storia può rappresentare una sorta di minaccia per la privacy. I progettisti dei sistemi devono attentamente bilanciare la necessità di accountability e il diritto alla privacy, controllando il modo e quando i dati vengono conservati e chi potrà analizzarli e recuperarli. Tra le tecniche che i database possono utilizzare per gestire in modo più sicuro la *storia* troviamo: la valutazione della conservazione non intenzionale dei dati nei sistemi esistenti, che possono minacciare la privacy, la riprogettazione dei componenti dei sistemi per evitare la memorizzazione non voluta dei dati e lo sviluppo di un nuove funzioni del sistema per supportare l'accountability. Nei database le impostazioni sulla privacy rappresentano un fattore critico: nei database responsabili si dovrebbero eliminare i dati scaduti in modo tempestivo, rimuovere la cronologia delle attività dal deposito, permettere agli utenti di monitorare in modo efficiente e sicuro i propri dati sensibili [15].

1.7.3 Sistemi distribuiti

PeerReview, fornisce un'accountabillity nei sistemi distribuiti. Assicura che un nodo corretto possa difendersi da false accuse; queste garanzie risultano essere molto importanti per i sistemi che si estendono su più domini amministrativi, che potrebbero non fidarsi a vicenda. PeerReview funziona mantenendo una registrazione sicura dei messaggi ricevuti e mandati da ciascun nodo. I record è utilizzato per rilevare automaticamente quando il comportamento di un nodo devia da quello determinato, individuando così i nodi difettosi. PeerReview è ampiamente applicabile: richiede solamente che le azioni di un nodo corretto siano deterministiche, che i nodi possano firmare i messaggi e che ogni nodo sia controllato periodicamente da uno corretto [16].

1.7.4 Content Delivery Network

Repeat and Compare, è un sistema per garantire l'integrità dei contenuti in un Content Delivery Network peer-to-peer non sicuro, anche quando le repliche generano dinamicamente contenuti. Rileva il comportamento anomalo delle repliche attraverso l'attestazione dei record e facendo leva sulla rete peer-to-peer per ripetere le generazione dei contenuti sulle altre repliche per poi confrontare i risultati [17].

Capitolo 2: Cloud Computing

Per *Cloud Computing* si intende un insieme di tecnologie che permettono all'utente di memorizzare, archiviare ed elaborare dati ed informazioni attraverso risorse (hardware o software) disponibili e virtualizzate su Internet.
Si riferisce quindi sia alle applicazioni fornite come servizio attraverso Internet, sia all'hardware e al software nei data center usati per implementare questo servizio.
Riprendo la definizione in [19] data da McKinsey e Co. Report, il Cloud Computing può essere definito come: *"…hardware-based services offering compute, network and storage capacity where: hardware management is highly abstracted from the buyer, buyers incur infrastructure costs are variable OPEX, and infrastructure capacity is highly elastic*[15]*"*.

Le sue definizioni sono numerose, ma possiamo individuare alcuni punti comuni a tutte:

- Si tratta di un servizio pay-per-use, quindi nessuna commissione ma semplicemente prezzi in base al reale utilizzo;
- Le risorse sono virtualizzate ed astratte;
- È presente un'interfaccia self-service;
- È caratterizzato da una forte capacità elastica (scale up/down su richiesta).

[15] "..sono servizi basati su hardware che offrono computazione, rete e capacità di archiviazione dove: la gestione dell'hardware è altamente astratta dall'acquirente, gli acquirenti sostengono costi di infrastrutture e operativi variabili e la capacità delle infrastrutture è elastica.

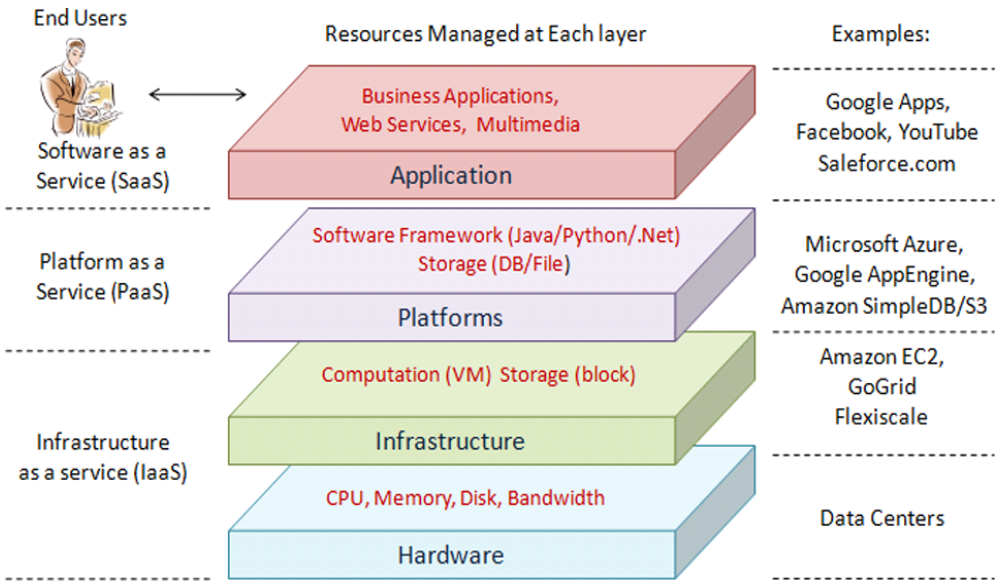

Figura 3: Architettura del Cloud Computing [18]

Come si vede dalla figura 3, il cloud computing adotta un modello di business basato sui servizi. In altre parole i livelli dell'infrastruttura, della piattaforma e delle applicazioni possono essere forniti come servizi *on demand*, raggruppati in tre categorie: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS).

Comparata con una tradizionale server farm, l'architettura del cloud computing è sicuramente più modulare. Ogni livello non è fortemente legato a quelli vicini, permettendo così ad ognuno di essi di evolversi separatamente. È molto simile allo stack OSI per i protocolli di rete. La modularità dell'architettura permette al cloud computing di supportare una vasta gamma di requisiti delle applicazioni pur mantenendo un overhead di gestione e manutenzione basso.

L'architettura del cloud computing può essere suddivisa in quattro livelli distinti: hardware, infrastruttura, piattaforma, applicazioni.

Analizziamoli più nello specifico.

2.1 Hardware

In questo livello troviamo le risorse fisiche del cloud: server, router, switch, sistemi di alimentazione e di raffreddamento. In pratica l'hardware è tipicamente implementato in un data center, che può contenere migliaia di server, organizzati in rack[16] e interconnessi tramite router, switch o altri dispositivi. Analizziamo quindi i componenti fondamentali di questo livello.

2.1.1 Server

I server sono organizzati in rack e ognuno di questi può contenere fino a 42 server in formato classico e fino a 128 nel più nuovo formato blade[17]. Tipicamente ogni server ha schede madri con più socket per ospitare varie cpu multi-core (fino a 10) e molti GB di RAM. Alcuni esempi di CPU possono essere gli Intel Xeon o gli AMD Opteron.

Figura 4: Rack [50]

2.1.2 Network

La pianificazione dell'architettura di rete è critica, visto che andrà ad influenzare notevolmente le performance delle applicazioni ed il throughput[18] dell'ambiente di calcolo distribuito. Tipicamente si adotta un'organizzazione a tre livelli:

- *Access Layer*: i server nei rack hanno accesso fisico alla rete e sono connessi ad uno switch con un collegamento a 1 Gbps. Questi sono connessi, tramite collegamenti a 10 Gbps, a due switch del livello successivo, cosi da essere tolleranti ad eventuali guasti.

[16] Tradotto letteralmente "armadi"
[17] Tradotto "lama", chiamati così per la loro forma sottile.
[18] Banda passante

- *Aggregation Layer*: questo livello fornisce importanti funzioni tra cui servizi di dominio, locazione e bilanciamento del carico. Ogni switch è collegato a più router del livello successivo, sempre per garantire una tolleranza ai guasti
- *Core Layer*: in questo livello i router gestiscono il traffico in uscita e in entrata dal data center. Generalmente vengono usati diversi ISP [19] per garantire una continuità della connessione.

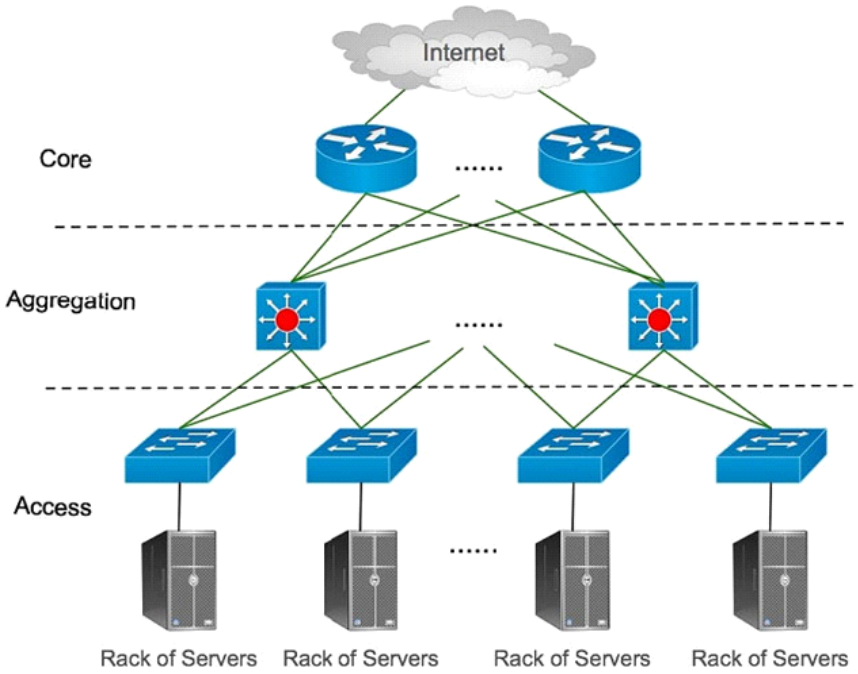

Figura 5: Design di base dell'infrastruttura di rete di un data center [18]

Come si vede dalla figura 5, tutti i collegamenti sono ridondanti per essere il più possibile tolleranti ai guasti delle apparecchiature di rete, dei server, dei collegamenti e perfino degli ISP.

La progettazione di un data center dovrebbe essere fatta in modo da raggiungere i seguenti obiettivi:

- *Uniform high capacity:* La velocità del traffico di rete tra due server dovrebbe essere limitata solo dalla capacità delle schede di rete del mittente e del destinatario. Ogni host presente nel data center dovrebbe essere in grado di comunicare con ogni altro host alla massima velocità.

[19] Internet Service Provider

- *Free Virtual Machine migrate*: La virtualizzazione permette di spostare l'intera VM, compreso il suo stato, da un server fisico ad un altro. La topologia di rete dovrebbe essere disegnata per supportare una veloce migrazione delle macchine virtuali.
- *Resiliency*: L'infrastruttura deve essere tollerante a varie tipologie di guasti ai server o ai collegamenti di rete. Le comunicazioni non dovrebbero essere influenzate, entro certi limiti, dai collegamenti fisici sottostanti.
- *Scalability*: L'infrastruttura di rete deve essere in grado di supportare un grande numero di server e consentire un'espansione incrementale.
- *Backward compatibility*: L'infrastruttura di rete dovrebbe essere compatibile con gli switch ed i router basati su Ethernet e IP, visto che molti data center hanno sfruttato queste tecnologie [18].

2.1.3 Alimentazione

Per garantire la continuità del servizio, i data center, oltre ad essere collegati alla normale rete elettrica, hanno diversi generatori che entrano in funzione in caso di guasti alla linea principale. Questi generatori, tipicamente diesel, richiedono alcuni secondi per l'avvio e per questo e altri motivi è necessario avere dei gruppi di continuità (UPS).

Gli UPS (*Uninterruptible Power Supply*) si trovano tra l'allacciamento alla rete elettrica ed i distributori di potenza (PDU) all'interno del data center.

La rete elettrica è tipicamente in corrente alternata (AC), così come all'interno del data center; mentre le batterie vengono caricate con corrente continua (DC) .

Attraverso questo ciclo AC-DC-AC si riescono ad eliminare i picchi o i cali di tensione che potrebbero arrivare dalla rete elettrica e che potrebbero danneggiare i componenti elettronici all'interno del data center. Tipicamente la batteria interna riesce a fornire energia per un breve periodo di tempo, ma questo è sufficiente per permettere ai generatori di emergenza di entrare in funzione, in caso di guasti alla linea principale.

I PDU (*Power Distribution Unit*) invece sono dispositivi atti a distribuire la corrente ai rack o agli apparati di rete all'interno del data center. Se ne possono trovare di due tipologie: i primi, abbastanza rari, simili a degli armadi e molto costosi, ricevono una o più linee ad alta tensione e la dividono in un qualsiasi

numero di linee a bassa tensione. L'altro tipo di PDU, quello più usato, è allocato all'interno dei rack e distribuisce la corrente ai server all'interno di questi e ai dispositivi di rete. Generalmente prendono come input una tensione più alta e la rendono disponibile in output attraverso delle normali prese di corrente. Alcuni PDU hanno anche funzioni per il monitoraggio remoto attraverso SSH[20], Telnet[21] o addirittura delle pagine web, permettendo così agli amministratori di controllare i carichi di corrente, lo stato e di accendere o spegnere una singola presa di corrente in uscita dal PDU. Questo può essere molto utile in una macchina remota, che per esempio ha smesso di rispondere e dev'essere riavviata: l'amministratore può collegarsi direttamente al PDU al quale il server è collegato, togliere la corrente dalla presa, forzare lo spegnimento della macchina e ridare successivamente corrente per farla ripartire.

Figura 6: Power Distribution Unit [23]

In un data center convenzionale l'energia viene fornita e distribuita dalla rete elettrica in corrente alternata, nonostante la maggior parte dei componenti elettrici e le batterie dei gruppi di continuità lavorino in corrente continua. In questo modo la corrente deve sottoporsi a varie conversioni, con il risultato di uno spreco di energia ed una perdita di potenza. Per ridurre il numero di conversioni della corrente e per avere una maggiore efficienza energetica del data center, evitando così il raffreddamento dei dispositivi, si sta sperimentando un allacciamento in corrente continua a 380V. Alcuni test hanno comparato queste strutture con quelle tradizionali che ricevono corrente a 480V DC, dimostrando che si può arrivare a una riduzione del 7% dell'energia consumata [20]. Ovviamente, per le strutture già

[20] Secure Shell, protocollo di rete per connessioni remote sicure
[21] Protocollo per login remoto, ormai sostituito da SSH

esistenti sarebbe necessario un adattamento dei dispositivi utilizzati e quindi un notevole investimento.

2.1.4 Raffreddamento

Il sistema di raffreddamento è molto importante in un data center, perché i componenti elettrici, lavorando, si surriscaldano e temperature troppo elevate possono condurre a malfunzionamenti o guasti.
Risulta inoltre opportuno mantenere un corretto tasso di umidità: se troppo elevato, può portare a condense all'interno delle apparecchiature; se troppo basso, può portare a scariche di elettricità statica.
Quindi la temperatura e l'umidità ambientale vengono rigorosamente controllate attraverso condizionatori e l'intera struttura è progettata per minimizzare la miscelazione di aria calda che esce dai server e quella fredda usata per raffreddarli. Questo fenomeno viene chiamato *corto-circuito*.

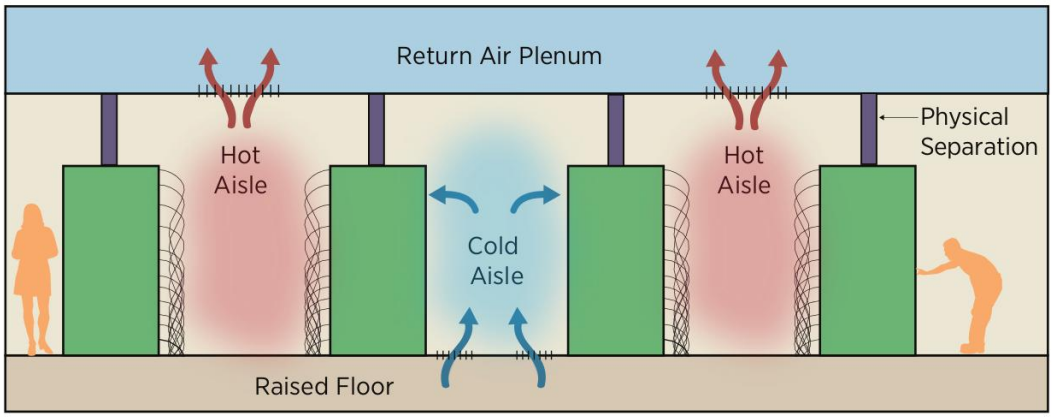

Figura 7: Sistema di raffreddamento e ciclo dell'aria [20]

Come mostra la figura, tipicamente si ha un piano rialzato che permette all'aria fredda di circolare tra questo ed il pavimento e di uscire attraverso delle piastrelle appositamente perforate poste in corrispondenza dei rack.
Questo spazio è utile anche per far passare i cavi di alimentazione o di rete, che però possono interferire con il flusso d'aria se non viene attuato un piano di manutenzione per rimuovere cavi inutilizzati o per disporli in modo ottimale.

Per minimizzare il ricircolo d'aria spesso vengono create *corsie fredde*, dove i server prendono in ingresso l'aria dei condizionatori, e *corsie calde,* dove l'aria viene espulsa dai server. Tutti i dispositivi sono installati in modo da garantire un flusso d'aria che entra dalla parte frontale del rack, (corsia fredda) ed esce dalla parte posteriore (corsia calda), non dimenticando che le file di rack devono essere poste "retro contro retro".

Per aumentare maggiormente questa separazione di temperature vengono spesso installate anche delle pareti isolanti, tipicamente in plastica, come quelle che si possono trovare nel reparto frigo dei supermercati, al di sopra delle file di rack.

Questi accorgimenti aiutano a ridurre la richiesta energetica delle ventole usate per raffreddare, di circa il 20-25% [20].

Per muovere l'aria nel data center si possono usare, in alternativa, più unità CRAC[22] (*Computer Room Air Conditioning*) dislocate in vari punti della struttura, oppure un'unica unità centralizzata. È stato però dimostrato che quest'ultima, dotata di un motore e di ventole di grandi dimensioni, è più efficiente rispetto a tante piccole unità CRAC, che "lottano" tra di loro per mantenere il tasso di umidità desiderato[23]. [20]

Le unità CRAC, fanno passare l'aria calda attraverso acqua fredda o liquidi refrigeranti così da raffreddarla, per poi riutilizzarla all'interno del data center.

Se il data center è situato in una zona molto fredda è possibile usare l'aria proveniente dall'esterno per raffreddarlo.

Vengono costantemente ricercarti nuovi modi per raffreddare queste enormi strutture. Ad esempio, Google nel 2009 ha acquisito una vecchia cartiera ad Hamina in Finlandia, che disponeva di un collegamento con il mare, per trasformarla in un data center e poter utilizzare l'acqua fredda proveniente dal Golfo di Finlandia. La costruzione del data center e l'adattamento della struttura esistente ha richiesto grosse sfide, ma è diventata una delle strutture più avanzate ed efficienti di Google [21].

Il miglioramento dell'efficienza energetica è una delle maggiori sfide per il cloud computing: è stato infatti stimato che il costo dell'alimentazione e del raffreddamento gravano per il 53% sulle spese di un data center.

[22] Più in generale unità HVAC, "Heating, Ventilation and Air Conditioning"

[23] Ad esempio un'unità deumidifica l'aria, mentre quella adiacente sta allo stesso tempo la sta umidificando, sprecando quindi energia.

Nel 2006 i data center in USA consumavano più dell' 1,5% di tutta l'energia generata annualmente ed è previsto che questa percentuale sia destinata a crescere ogni anno del 18%. [22]

I provider delle infrastrutture sono sotto pressione per ridurre questi consumi, ma lo scopo non è solo quello di diminuire i costi, ma anche quello di adempire alle leggi e agli standard ambientali. Per questo motivo la progettazione di data center efficienti sta ricevendo sempre più attenzione.

Per raggiungere questo obiettivo si possono usare diversi accorgimenti:

- adottare architetture hardware capaci di diminuire la velocità di una CPU se non utilizzata;
- lo spegnimento di alcuni componenti non utilizzati o di alcune parti;
- la schedulazione di processi energy-aware;
- la consolidation dei server, cioè quando molti server piccoli sono sostituiti da un server più grande e il software delle vecchine macchine viene virtualizzato in quella nuova.

Recenti ricerche hanno iniziato a studiare anche protocolli e infrastrutture di rete sensibili al consumo. La sfida in tutti questi metodi è quella di raggiungere un trade-off tra il risparmio energetico e le performance delle applicazioni.

2.1.5 Data Center modulari (MDR)

Un'alternativa ai tradizionali data center sono i data center modulari (MDR): container che possono essere trasportati e posizionati in qualsiasi parte del mondo, in base alle necessità; possono essere aggiunti ad altri data center esistenti, sia modulari che non, oppure posizionati in punti strategici. Un MDR può essere installato ovunque ci sia un collegamento alla rete elettrica e idrica ed una connessione a Internet.

Tipicamente gli MDR sono costituiti da circa 200 server, con le apparecchiature di rete e il sistema di raffreddamento necessari.

Questi data center possono essere utili:

- in situazioni di emergenza, per esempio per le organizzazioni che devono coordinare i soccorsi;
- per operazioni militari;

- per offrire supporto a quelli tradizionali, posizionandoli vicino ad aree densamente popolate o ad aziende che utilizzano applicazioni altamente interattive e che sono sensibili ai tempi di risposta.

I data center modulari presentano i seguenti vantaggi:

- rapida installazione
- alta efficienza energetica
- computazione intensiva
- prezzi contenuti
- riduzione significativa dei tempi di costruzione, da svariati anni a qualche mese.

I problemi tipici di questo livello comprendono la configurazione hardware, la gestione del traffico, dell'energia e del raffreddamento.

Figura 8: Modular Data Center [24]

2.2 Infrastruttura

Questo livello, definito anche della virtualizzazione, crea un pool di risorse partizionando le risorse fisiche tramite tecnologie di virtualizzazione come Xen, KVM e Vmware.

Il livello dell'infrastruttura è una componente fondamentale del cloud computing, dato che alcuni aspetti chiave, come l'assegnamento dinamico delle risorse, sono disponibili solo attraverso tecnologie di virtualizzazione.

2.2.1 Virtualizzazione

È la possibilità di astrarre le componenti hardware di un computer al fine di renderle disponibili al software in forma di risorse virtuali.
È una tecnologia che permette di nascondere i dettagli dell'hardware e che fornisce risorse virtualizzate per le applicazioni di alto livello. Un server virtualizzato è comunemente chiamato *virtual machine* (VM).
Questa tecnologia è fondamentale nel cloud computing, visto che fornisce le capacità necessarie per mettere in comune le risorse computazionali di un cluster e di assegnarle o riassegnarle alle applicazioni, su richiesta.
Su una macchina fisica è possibile eseguire più sistemi operativi virtualizzati contemporaneamente, senza avere la necessità che il sistema operativo sia compatibile con l'hardware sottostante, in quanto la VM crea un livello di astrazione. Quest'ultima può essere facilmente clonata e spostata (migrata) su un altro server in base alle necessità ad esempio per bilanciare il carico all'interno del data center.
Recentemente Xen e Vmware hanno implementato una migrazione *live*, dove lo spostamento della virtual machine può avvenire in un tempo estremamente contenuto, nell'ordine delle decine di millisecondi fino ad un secondo [18].

2.2.2 File system distribuiti

Un file system distribuito è un qualsiasi file system che permette l'accesso ai file da più computer che condividono una rete, rendendo possibile la condivisione di file e di risorse di archiviazione.
L'esempio più rilevante è sicuramente *Google File System:* il file system progettato, realizzato e distribuito dal colosso americano per fornire un efficiente ed affidabile accesso ai dati quando si utilizza una grande infrastruttura cluster.
Il cluster nel Google File System è costituito da numerosi nodi, che si suddividono in due tipologie: un *nodo Master* e un grande numero di nodi *Chunkserver*, che contengono i file divisi in chunk di 64 MB. Il nodo Master assegna un identificativo univoco a 64 bit ad ogni chunk al momento della loro creazione. Ognuno di essi è poi replicato diverse volte (almeno tre) attraverso la rete, specialmente i file che hanno una richiesta elevata o che hanno bisogno di ridondanza.

Il *Master server* non memorizza le parti di file, ma piuttosto tutti i metadati associati ad esse, come le tabelle che mappano gli identificativi a 64 bit alle locazioni di memoria, la posizione delle copie dei chunk e quali processi stanno scrivendo o leggendo quest'ultimo.

I Chunk server inviano periodicamente aggiornamenti al Master server per tenerlo costantemente aggiornato. La presenza di un unico Master permette di avere una visone globale e completa del sistema.

Le modifiche dei file sono gestite da un sistema dove il Master server concede ai chunk server, per un periodo limitato di tempo, i permessi per modificare una determinata parte di file, non permettendo a nessun altro processo di accedervi.

Il server proprietario del chunk modificato propaga i cambiamenti a tutti gli altri server con le copie di backup. Le modifiche non sono salvate fino a quando tutti i server non garantiscono il compimento dell'operazione.

I programmi accedono al chunk dopo aver ottenuto dal server Master la posizione del chunk desiderato.

In confronto ai tradizionali file system, GFS è progettato e ottimizzato per fornire un elevato throughput, una bassa latenza e per sopravvivere all'eventualità di errori in singoli server. Le performance di Google File System in lettura, quando usato su un ridotto numero di server, sono comparabili a quelle di un normale hard disk, mentre quelle in scrittura o di aggiunta alla fine di un file, sono abbastanza scarse. Visto che il *Master node* non è chiamato in causa in queste operazioni, le performance vengono incrementate notevolmente all'aumentare dei chunk server utilizzati. Per esempio utilizzando 342 nodi, si arriva a una velocità in lettura di 583 MB/s [25].

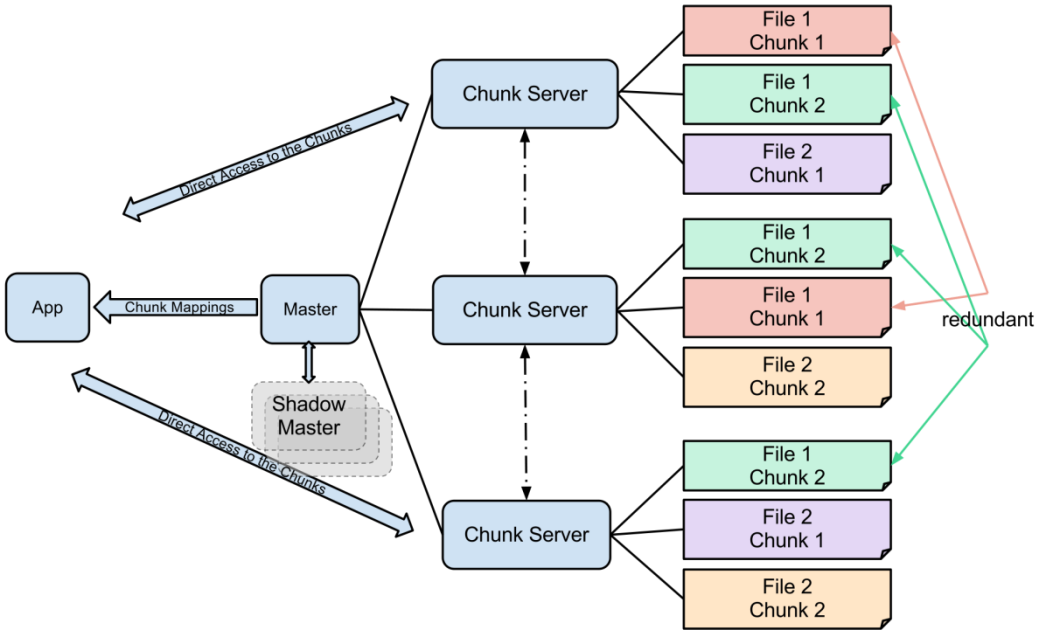

Figura 9: Google File System da Wikipedia

Oltre al GFS, è rilevante anche l'*Hadoop Distributed File System* (HDFS): un file system distribuito open source ispirato a quello di Google. Similmente a quest'ultimo, nell'HDFS i dati sono salvati in diversi nodi.

Il file system è costruito attraverso un cluster di *datanode*, ognuno dei quali serve blocchi di dati attraverso la rete usando un protocollo specifico.

I dati sono anche disponibili attraverso il protocollo HTTP, permettendo l'accesso a tutti i contenuti attraverso un web browser. I nodi possono comunicare tra di loro per bilanciare la distribuzione dei dati, per spostare copie o per mantenere elevata la ridondanza dei dati. Il file system utilizza il protocollo TCP/IP per comunicare, i client invece usano RPC. HDFS ha un *single point of failure*[24] e non garantisce un'alta disponibilità, perché una sua istanza richiede un unico server, il *namenode*, e quindi se quest'ultimo si guasta tutto il file system diventa irraggiungibile.

Quando il nodo ritorna disponibile dopo un malfunzionamento, deve ripetere tutte le operazioni in sospeso e questo processo può durare anche trenta minuti per cluster di grosse dimensioni. Esiste anche un *secondary namenode* che periodicamente fa degli *snapshot*[25], cosi da poter ripartire da questi "punti di

[24] Single point of failure, significa che è presente un unico componente vulnerabile, che in caso di malfunzionamento o anomalia causa il blocco dell'intero sistema

[25] È una "fotografia", una copia del sistema in un particolare momento.

salvataggio", quando quello principale si guasta, invece di dover ripetere tutte le operazioni.
Visto che il namenode è l'unico punto di salvataggio e gestione dei metadati, questo può diventare un collo di bottiglia, soprattutto con numerosi file di piccole dimensioni [26].

2.2.3 Database distribuiti

Per gestire l'elevata quantità di dati disponibili in un ambiente cloud, nascono i *database distribuiti*, che rendono possibile un accesso veloce ai dati su un ampio numero di nodi.
Un database distribuito, al contrario di uno tradizionale, è composto da diversi computer, che possono essere situati nella stessa struttura, ma molto spesso anche in strutture diverse, permettendo anche di replicare i dati, per aumentarne le performance.
Alcuni esempi importanti sono Google BigTable, la sua versione open source HBase, Amazon Dynamo e Windows Azure Storage.

Google BigTable

Google BigTable è un database management system proprietario, altamente coerente e compresso e ad alte prestazioni costruito sul Google File System e su alcune altre applicazioni di Google. È progettato per scalare da poche macchine fino a centinaia o migliaia di server con petabyte[26] di dati e viene sfruttato da più di una sessantina di prodotti Google, tra cui Google Earth, Google Maps, Google Code e YouTube. Queste applicazioni fanno richieste molto diverse tra loro, sia in termini di dati richiesti (URL, pagine web, immagini satellitari), sia di requisiti di latenza (dati real-time, computazione di backend), ma nonostante questo il sistema è flessibile e ha delle buone performance.
BigTable non è un database relazionale e può essere meglio definito come una mappa persistente, multidimensionale e distribuita. La mappa è indicizzata attraverso una chiave per le righe, una per le colonne e un timestamp a 64 bit (tutti questi valori sono array di byte non interpretati)

[26] 1 milione di gigabyte

In una tabella, le chiavi di riga sono stringhe arbitrarie ed ogni lettura o scrittura di una singola riga è un'operazione atomica.

BigTable mantiene un ordine lessicografico per chiave di riga, rendendo cosi la lettura di un piccolo range di chiavi più efficiente e coinvolgendo un ridotto numero di macchine. Per esempio le pagine web di uno stesso dominio sono raggruppate in righe adiacenti invertendo le componenti degli URL[27].

Salvare pagine dello stesso dominio vicine, permette un analisi più efficiente degli host e dei domini.

Le tabelle sono ottimizzate per essere usate sul GFS, vengono divise in *tablet*, cioè gruppi di righe di circa 200 MB ciascuno. Quando le dimensioni iniziano ad aumentare, i tablet vengono compressi. Le posizioni dei tablet nel GFS vengono inserite nel database, in tablet speciali, chiamati *META1*.

I tablet META1 vengono trovati facendo una query[28] all'unico tablet, META0, che si trova in un server separato, visto che riceve numerose richieste. Questo però non crea un collo di bottiglia perché le richieste che riceve non richiedono una grande computazione o molta banda; inoltre sia META0 che i vari META1 e i client, fanno largo uso di cache[29] e pre-fetching[30]. Google BigTable è accessibile unicamente attraverso *Google App Engine* [27].

Hbase

Hbase, come già accennato, è un database distribuito, open source e ispirato a Google BigTable. È compresso, orientato alla colonna, scalabile e consistente. È sviluppato dall'*Apache Software Foundation* e viene eseguito su HDFS, fornendo le stesse funzionalità di BigTable.

Facebook, a novembre 2010, ha scelto di usare questo dabatase per il suo nuovo sistema di messaggistica [28].

Amazon Dynamo

Amazon Dynamo è un database distribuito, proprietario, *eventually consistent*[31] che viene eseguito su un cluster di centinaia di computer Linux, collegati ad una

[27] Esempio: maps.google.com viene salvato come com.maps.google
[28] Interrogazione al database
[29] Memoria temporanea
[30] Tecnica in cui vengono caricati preventivamente i dati in memoria cache
[31] È un termine usato nella programmazione parallella e significa che trascorso un periodo abbastanza lungo di tempo, in cui non c'è stato alcun cambiamento, ci si aspetta che le modifiche siano propagate in tutto il sistema, copie comprese

rete interna. Dato che non viene venduto come pubblico servizio e quindi il sistema non è progettato per essere esposto su Internet, gli sviluppatori ritengono che non vi sia la necessità di concentrarsi sulla sicurezza, cosi da focalizzarsi solo sulle performance, sulla reattività e sulla disponibilità di servizio [29].
Dynamo è utilizzato da diverse applicazioni di Amazon, tra cui Amazon Simple Storage Service.

Apache Cassandra

Apache Cassandra riunisce le tecnologie dei sistemi distribuiti di Dynamo ed i modelli di dati di BigTable. Come il primo, è *eventually consistent*, mentre come il secondo fornisce un modello di dati basato su famiglie di colonne, più ricco di un tipico sistema chiave/valore.
Cassandra fornisce un sistema chiave/valore strutturato, dove le chiavi mappano valori multipli, che sono raggruppati in famiglie di colonne, prefissate al momento della creazione del database, ma le colonne possono essere aggiunte ad una famiglia in ogni istante [30].
Inoltre le colonne sono aggiunte solo alle chiavi specificate, così quelle diverse possono avere un numero di colonne differente. Siccome i valori di ogni famiglia di colonne per ogni chiave sono salvati insieme, Cassandra risulta essere un sistema DMBS[32] ibrido fra uno orientato alle colonne ed uno orientato alle righe. Una tabella, in questo database, è una mappa multidimensionale distribuita, indicizzata da una chiave. Il valore è un oggetto altamente strutturato. La chiave di una riga è una stringa di lunghezza arbitraria e le operazioni per ogni singola riga sono atomiche, indipendentemente dal numero di colonne che vengono lette o scritte. Non esiste un *single point of failure*, visto che i nodi sono tutti identici.
Apache Cassandra è stato sviluppato inizialmente da Facebook che dal 2008 ne ha rilasciato il codice sorgente; in seguito è diventato uno dei top-project di Apache. Facebook ha abbandonato Cassandra in favore di HBase alla fine del 2010.

2.2.4 Framework

Un framework è un'astrazione nella quale il software fornisce funzionalità che possono essere usate da altri programmi, tramite librerie.

[32] Database Management System

MapReduce

MapReduce è un framework sviluppato da Google per supportare la computazione distribuita su grandi insiemi di dati risiedenti in un cluster, sia in database che in file system. Si ispira alle seguenti funzioni della programmazione funzionale:

- *Map*: Il master node prende l'input, lo divide in problemi più piccoli e lo distribuisce ai nodi. Un nodo potrebbe fare a sua volta questa operazione, creando cosi una struttura ad albero multilivello.
- *Reduce*: Il master node riceve le risposte di tutti i sottoproblemi, li combina e li fornisce come output: questa rappresenta la risposta al problema iniziale.

MapReduce permette una computazione distribuita delle due operazioni. Se le funzioni di mappatura sono indipendenti le une dalle altre, tutti i processi di map possono essere eseguiti in parallelo, nonostante questo sia in pratica limitato dal numero di dati indipendenti e dal numero di cpu/core disponibili nelle macchine vicine alla sorgente dei dati.

In modo simile, un insieme di operazioni di reduce possono essere eseguite insieme se tutti gli output delle operazioni di map, che condividono la stessa chiave, sono disponibili contemporaneamente.

Sebbene questo processo possa sembrare lento paragonato ad algoritmi più sequenziali, MapReduce può essere applicato a database di grandi dimensioni: per esempio può ordinare petabayte di dati in poche ore.

Il parallelismo offre anche meccanismi di recupero in caso di errore: se uno dei "mappatori" o dei "riduttori" fallisce, o se non risponde entro un tempo prefissato, il suo lavoro può essere rischedulato, assumendo che i dati siano ancora disponibili [31].

Hadoop MapReduce

Hadoop MapReduce è la versione open source di Google MapReduce. È presente un *JobTracker* al quale le applicazioni client inviano i processi di MapReduce e che invia il "lavoro" ai nodi *TaskTracker*, cercando di tenere i processi il più possibile vicino ai dati. Con il file system rack-aware, il JobTracker è a conoscenza di quale nodo contiene i dati e quali altre macchine sono vicine. Se il lavoro non può essere eseguito sulla stessa macchina in cui risiedono i dati, la priorità viene data ai nodi nello stesso rack, cosi da ridurre al minimo il traffico

nella rete. Se un nodo TaskTracker fallisce o va in time out il processo viene rischedulato.

Un *heartbeat*[33] viene spedito regolarmente dal TaskTracker ai JobTracker per controllare il loro stato. Nelle ultime versioni, sono stati introdotti dei checkpoint in cui viene salvato lo stato dei JobTracker, in modo da non dover ricominciare l'intero lavoro in caso di malfunzionamenti.

Molte aziende utilizzano il framework di Hadoop, per esempio AOL, Apple, eBay, IBM, Facebook, foursquare, ImageShack, Last.fm, LinkedIn, Microsoft, Netflix, The New York Times, StumbleUpon, Twitter e Yahoo!.

Nel luglio 2011, Facebook ha reso noto di avere il più grande cluster di Hadoop con 30 PB di dati. Amazon invece attraverso il framework fornisce il proprio servizio di MapReduce: *Amazon Elastic MapReduce* [32].

2.2.5 Esempi Infrastrutture

Amazon Elastic Compute Cloud (Amazon EC2) permette agli utenti di eseguire e gestire istanze di server in un data center, usando delle API[34] o dei *tool* e delle *utilities*. Le istanze di EC2 sono delle Virtual Machine eseguite sulla Xen Virtualization Engine, e funzionano come *virtual private server*[35]. Dopo aver creato un'istanza, un utente può caricare i propri programmi, fare le proprie personalizzazioni, ed infine creare un'immagine di partenza. Copie identiche di questa immagine possono essere eseguite sulle Virtual Machine in ogni momento. L'utente ha praticamente il controllo completo sull'istanza, che si comporta come hardware e di conseguenza per Amazon diventa difficile offrire un ridimensionamento automatico delle risorse. È possibile creare, lanciare e terminare istanze di server a seconda della necessità, pagando le ore di effettivo utilizzo (da qui il termine *elastic* del nome). L'utente può decidere dove posizionare la propria istanza, cosi da poter gestire al meglio le latenze e la ridondanza [33].

Flexiscale e *GoGrid* sono atri due esempi di IaaS cloud provider e come Amazon EC2 permettono di creare Virtual Machine e di eseguirle al momento del bisogno.

[33] Letteralmente "battito del cuore", inteso come un operazione che viene ripetuta periodicamente
[34] Application Programming Interface
[35] È un termine usato per chiamare le virtual machine, enfatizzando che è equivalente a un computer fisico, completamente dedicato all'utente.

L’utente paga per l'uso effettivo che ne viene fatto, tipicamente a ore, ed è possibile anche comprare solo una risorsa specifica, per esempio aumentare la RAM disponibile. Entrambi i servizi offrono sia Linux che Windows ed un comodo pannello di controllo web, da cui è possibile aggiungere o rimuovere le risorse. Flexiscale è stato il primo provider europeo e il secondo a livello mondiale, dopo Amazon. [34, 35]

Degni di nota sono anche *Eucalyptus* e *OpenStack:* entrambi progetti open source, sono software per l'implementazione di cloud attraverso cluster di computer. Eucalyptus è l'acrononimo di *Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems* ed è più orientato alla progettazione di cloud privati o ibridi. Presenta molti partner tra cui Dell, HP, Intel, Novell e RedHat, è supportato dalle maggiori distribuzioni Linux, inculse Debian, RedHat, SUSE Linux, Ubuntu e Fedora ed è supportato da varie tecnologie di virtualizzazione tra cui Vmware, Xen e KVM. Ubuntu fino a ottobre 2011 usava Eucalyptus per offrire Ubuntu Enterprise Cloud, per poi passare a OpenStack, garantendo però ancora il supporto [36].

OpenStack invece è un progetto di IaaS cloud computing di RackSpace Cloud e della NASA, rilasciato sotto licenza Apache. Al momento circa 120 compagnie fanno parte di questo progetto, incluse AT&T, Dell, AMD, Intel, Canonical, Reddit, SUSE Linux, HP e Cisco. Lo scopo di questo progetto è quello di permettere a qualsiasi organizzazione di creare ed offrire servizi di cloud computing, usando hardware standard [37].

2.3 Piattaforma

Il livello della piattaforma è costruito sopra il livello dell'infrastruttura, offre sistemi operativi, piattaforme e soluzioni software che aiutano a minimizzare l'onere di fare il deploy direttamente sulle VM. Inoltre si evitano i costi e le complessità di comprare e gestire l'hardware e il software sottostante. Per esempio Google App Engine opera a questo livello per fornire delle API di supporto per implementare logiche di storage, database e business tipiche delle web application.

2.3.1 Google App Engine

È la piattaforma per lo sviluppo e l'hosting di applicazioni web nei data center gestiti da Google, dove le applicazioni vengono eseguite in *sandbox*[36]. *Google App Engine* offre un ridimensionamento automatico delle risorse per le applicazioni, cioè vengono allocate risorse in base alla domanda. Questo processo viene gestito interamente dalla piattaforma e l'utente non può impostare nessun parametro. Si possono costruire applicazioni usando le tecnologie standard di Java come JVM, Java Servlet, il linguaggio Java o ogni altro linguaggio basato su interpreti o compilatori JVM come JavaScript o Ruby. È a disposizione anche un interprete Python e le relavitve librerie standard e *Go*, un linguaggio sviluppato da Google. Oltre alla proprie applicazioni è possibile utilizzare le Google Apps, personalizzandole e usando un proprio nome di dominio. Le piattaforme web eseguite su questa piattaforma includono GAE Framework, Django, CherryPy, web2py e webapp2. Gli sviluppatori hanno un accesso di sola lettura al file system, ma possono essere usati file system virtuali. Le applicazioni possono permettere agli utenti di autenticarsi tramite un account Google, così è molto probabile che non debbano creare un nuovo account per autenticarsi nell'applicazione [38].

2.3.2 Windows Azure Platform

Windows Azure Platform è la piattaforma di Microsoft per costruire, ospitare e scalare applicazioni web nei data center di Microsoft. È costituita da una varietà di prodotti che vengono raggruppati sotto i seguenti brand: Windows Azure, SQL Azure e Windows Azure AppFabric.

Windows Azure è un sistema operativo che fornisce computazione e storage scalabili. In pratica si tratta di un'astrazione per descrivere un certo numero di sistemi Windows Server che attraverso tecnologie di virtualizzazione forniscono i servizi di computazione (*Compute*) e archiviazione (*Storage*).

Compute è la componente che permette di eseguire effettivamente le applicazioni creando delle istanze di Virtual Machine. Una volta che le risorse vengono assegnate all'applicazione, Compute si occupa gestire il carico, scalando se necessario.

[36] Termine usato per riferirsi a un ambiente isolato dal resto del sistema

Sono disponibili tre ambienti di calcolo, in 'contenitori' chiamati *Role*, ognuno con scopi diversi:

1. *Web Role*, fornisce un web server IIS[37] dedicato usato per il frontend delle applicazioni web.
2. *Worker Role*, permette di eseguire applicazioni che non hanno necessariamente bisogno di interazione con l'utente. In pratica vengono eseguiti i processi in background o a lungo termine a supporto dei Web Role.
3. *VM Role*, abilita l'utente a usare una versione personalizzata di Windows Server per quelle applicazioni, spesso datate, che richiedono un alto numero di personalizzazioni del sistema operativo e non possono essere eseguite direttamente sul cloud.

Windows Azure Platform supporta applicazioni costruite con il framework .NET e i tipici linguaggi di programmazione supportati da Windows, come C#, C++, Visual Basic.

La componente *Storage* offre tre alternative per archiviare dati in strutture non relazionali:

1. BLOB (Binary Large Object), per salvare una grande quantità di dati non strutturati come documenti, video, immagini o file binari.
2. Table, usato per salvare grandi quantità di dati che necessitano una struttura. Non fornisce però alcun modo per relazionare dati tra loro.
3. Queue, un modo affidabile per trasmettere messaggi tra applicazioni o servizi all'interno della piattaforma.

SQL Azure è la versione scalabile, per il cloud, di SQL Server. Gli utenti non devono installare o gestire il database e possono limitarsi a usare le funzionalità del database relazionale.

Windows Azure AppFabric facilita la creazione e la distribuzione di applicazioni e le sue componenti principali sono:

- *Access Control Service*: fornisce un singolo punto di accesso per autenticare l'utente in tutte le applicazioni web e riduce al minimo la

[37] Internet Information Service

scrittura di codice e le conoscenze necessarie per implementare un servizio di autenticazione.

- *Service Bus*: fornisce un connessione sicura per comunicare nell'ambiente distribuito o tra questo e le applicazioni che l'utente utilizza localmente. Il servizio sceglie automaticamente il protocollo e i pattern per comunicare e assicura la consegna del messaggio, senza che l'utente se ne debba preoccupare [18, 39, 46]

2.3.4 Amazon Web Services

Amazon Web Services (AWS) è un insieme di decine di servizi Amazon che combinati tra loro possono fornire un servizio come piattaforma. Il punto centrale è il già citato Amazon EC2 che unito a Amazon Simple Storage Service (Amazon S3) e ad altri servizi a seconda delle necessità, permette il deploy e la gestione delle applicazioni nel cloud di Amazon. Un esempio di tali servizi può essere Amazon Relational Database Service (Amazon RDS), che offre le funzionalità di un database relazionale o Amazon SimpleDB, una database non relazionale. Amazon Simple Queue Service (Amazon SQS), invece, fornisce un servizio molto performante per distribuire il carico di lavoro fra le applicazioni [40].

2.3.5 Force.com

Un ultimo esempio è *Force.com*, un servizio PaaS di Saleforce.com, che permette un facile sviluppo di applicazioni web grazie a tool visuali che permettono di costruire le applicazioni "a blocchi", riducendo al minimo la scrittura di codice. Oltre a questo offre API per integrare applicazioni già sviluppate esternamente e un framework per creare un "social network" per lavorare efficientemente con i colleghi, dove si possono lasciare feedback, creare conversazioni e condividere file. Inoltre fornisce tool per costruire applicazioni e interfacce ottimizzate per i dispositivi mobili. Fra le compagnie che utilizzano Force.com si possono trovare Belkin, Groupon, Qualcomm e Häagen-Dazs [44].
Esiste anche la possibilità di usare Force.com insieme a Google App Engine per unire i pregi di entrambe le piattaforme [41].

2.4 Applicazioni

I cloud provider installano e gestiscono le applicazioni nel cloud e gli utenti accedono a queste attraverso dei client. Gli utenti non gestiscono l'infrastruttura e la piattaforma sottostanti, su cui le applicazioni vengono eseguite, anzi molto probabilmente ne ignorano l'esistenza. Questo elimina il bisogno di installare ed eseguire i programmi direttamente sui computer dei clienti, semplificando la manutenzione ed il supporto. La maggior parte delle applicazioni può essere raggiunta tramite un browser, anche se alcuni servizi offrono applicazioni leggere, per esempio per sincronizzare i file, oppure applicazioni appositamente progettate per smartphone e tablet. Quello che rende le applicazioni cloud diverse da quelle tradizionali è l'elasticità, cioè grazie alle tecnologie precedentemente descritte negli altri livelli, il lavoro viene distribuito su più server e scalato automaticamente, ottenendo performance migliori ed una maggiore disponibilità.

Il SaaS è diventato di uso comune tra le applicazioni aziendali per la collaborazione, l'accounting, la gestione delle relazioni coi clienti (CRM[38]), la pianificazione delle risorse (ERP[39]), la gestione delle risorse umane (HRM[40]) e la gestione dei contenuti (CM[41]) [42].

Questo livello contiene tutte le applicazioni usate dagli utenti. Servizi come Google Apps, Dropbox, iCloud, Netflix, Facebook, YouTube e praticamente tutte le applicazioni usufruibili attraverso un browser web, ricadono in questo livello.

Salesforce.com è un sistema di Customer Relationship Management pay-as-you-go attraverso Internet. Permette di usare la potenza del loro cloud per gestire le relazioni coi clienti, il team delle vendite e per tracciare i dati degli utenti .

Dropbox, Box.com, SkyDrive, SugarSync sono servizi di archiviazione remota in cui l'utente può salvare i propri file nel cloud e accedere ad essi tramite un qualsiasi browser web. Nel caso di Dropbox, si può anche installare un client per sincronizzare i file sul proprio computer. iCloud e Ubuntu One, oltre a sincronizzare i file, permettono di fare un backup delle impostazioni dell'utente e per esempio iCloud sincronizza anche i contatti, il calendario, i segnalibri, le note, ecc.

[38] Customer Relationship Management
[39] Enterprise Resource Planning
[40] Human Resource Management
[41] Content Management

Google Apps offre i comuni prodotti di Google in una versione personalizzabile e con la possibilità di scegliere un proprio nome di dominio. Comprende applicazioni come Gmail, Google Docs, Google Calendar che hanno funzionalità simili ad una normale suite da ufficio. Google Docs per esempio permette di creare e modificare documenti online e di collaborare in tempo reale con altri utenti. Per uno scopo simile è presente anche Google Cloud Connect, che permette di aggiungere un plugin alla suite di Microsoft Office per sincronizzare i propri documenti con Google Docs e sfruttarne tutte le funzionalità, come la collaborazione simultanea e la visualizzazione delle modifiche in tempo reale [43].

L'adozione del cloud computing porta sicuramente dei benefici, ma presenta anche alcuni ostacoli. Per esempio le aziende sono preoccupate riguardo alla disponibilità delle loro applicazioni e dei loro servizi e temono che possano essere irraggiungibili. Un altro ostacolo è l'interoperabilità delle piattaforme, costruendo le applicazioni per un particolare frame work può risultare difficile migrare verso un altro cloud provider.

Può risultare lento e costoso spostare grosse quantità di dati nel cloud, citando l'esempio riportato dall'Università di Berkeley, per trasferire 10 TB di dati dall'università ad un data center di Amazon si impiegherebbero 45 giorni con una connessione da 20 Mbit/sec, mentre spedendo 10 hard disk da 1 TB con un normale corriere si impiegherebbe meno di una giornata [7]. Un ultimo ostacolo è costituito dalla sicurezza e dalla privacy dei dati. A questo riguardo, sta emergendo il ruolo dell'accountability nei sistemi cloud, che verrà approfondito nel prossimo capitolo.

Capitolo 3: Accountability nel Cloud

3.1 Problematiche del Cloud

Il cloud computing richiede alle aziende e ai singoli individui di trasferire parzialmente o totalmente il controllo delle risorse al cloud service provider. Quest'azione pone naturalmente delle preoccupazioni sulle decisioni da prendere a riguardo. In una recente ricerca è stato scoperto che l'88% dei potenziali utilizzatori del cloud è preoccupato riguardo a chi potrà accedere ai propri dati ed alle attività svolte sui server fisici [45]. Nonostante i rischi possano essere attenuati attraverso un *controllo preventivo*, per esempio criptando i dati o controllando gli accessi, questo non sempre è sufficiente e a volte non è neanche possibile, ad esempio nel caso in cui sulle informazioni sia necessaria una computazione. È importante completare queste misure con altre altrettanto rilevanti, che promuovano la trasparenza, la governance e la responsabilità del cloud provider.

La ricerca dell'European Network and Information Security Agency (ENISA) sui rischi legati al cloud computing pone la perdita di governance tra le maggiori minacce soprattutto per le IaaS.

Sebbene l'*audit* sia una componente cruciale nella creazione di fiducia, i maggiori cloud provider non forniscono ancora una piena trasparenza e nemmeno gli strumenti necessari per un tracciamento ed un controllo della storia degli accessi ai file e della provenienza dei dati, sia delle macchine virtuali che di quelle fisiche utilizzate. Attualmente gli utenti possono al massimo monitorare i parametri delle macchine virtuali ed i log degli eventi dei servizi utilizzati.

Dal punto di vista del cliente, sebbene utilizzare il cloud possa apportare svariati benefici, può essere anche rischioso perché si deve rinunciare in larga misura al controllo sulla computazione e sui dati. In un modello convenzionale in cui il

calcolo viene eseguito in un data center, tipicamente presso la sede dell'azienda, il cliente ha accesso fisico ai server, può osservare il loro stato e può affidare la loro gestione a personale di fiducia. Nel nuovo modello, dove la computazione viene invece eseguita su macchine virtuali, nel cloud, l'utente non può svolgere nessuna delle azioni precedenti. La gestione della macchina fisica è delegata al *cloud provider* e l'utente può solamente gestire la macchina virtuale in remoto, attraverso una connessione.

La perdita di controllo diviene particolarmente critica all'insorgere di eventuali problematiche. Alcuni problemi che potrebbero verificarsi, secondo [47] sono:

- Le macchine nel cloud sono difettose o non adeguatamente configurate e potrebbero di conseguenza corrompere alcuni dati o restituire risultati non corretti, derivanti da una computazione errata.
- Il cloud provider potrebbe accidentalmente allocare meno spazio di quello necessario, portando ad un degrado delle performance o al mancato adempimento della SLA[42].
- Un hacker potrebbe sfruttare un bug nel software per rubare dati sensibili o prendere il controllo dell'intera macchina, per inviare spam o per fare attacchi di tipo DoS.
- L'utente potrebbe non aver accesso ai propri dati perché il cloud provider li ha persi o semplicemente perché non sono disponibili in quel momento.

Alcuni di questi problemi, come l'allocazione di risorse inadeguata, sono specifici del cloud e potrebbero non verificarsi in altri tipi di piattaforme; altri invece, come la perdita dei dati o la rottura di componenti hardware, sono problemi comuni e l'uso del cloud ne ha solo incrementato la gravità.

Per esempio, una macchina può essere difettosa sia in un normale data center, sia nel cloud: nel primo caso però il cliente può effettuare upgrade regolari e assumere tecnici capaci e di fiducia; nel cloud, invece, si deve affidare al provider. Purtroppo, poichè che le responsabilità di gestione sono suddivise tra il cliente e il provider, nè l'uno né l'altro si trova nella posizione ideale per affrontare questi problemi.

[42] Service Level Agreement, strumenti contrattuali per definire i termini del servizio.

Diventa quindi critica anche l'identificazione di un problema: da una parte vi è il provider che non sa precisamente cosa cercare, in quanto non è al corrente di ciò che dovrebbe fare l'elaborazione; dall'altra parte vi è invece il cliente che può accedere alla macchina solo in remoto, quindi ha a disposizione informazioni molto limitate.
Una volta riconosciuto il problema, le due parti devono attribuire correttamente le reciproche responsabilità: questa fase è spesso fonte di scontri difficilmente risolvibili da terze parti.
L'assenza di un metodo affidabile per individuare gli errori ed attribuire correttamente le responsabilità scoraggia i potenziali utilizzatori del cloud e complica l'uso di determinate applicazioni.

3.2 L'accountability come soluzione

L'accountability può essere una soluzione a questi problemi.
È importante prima di tutto ricordare alcuni concetti fondamentali dell'accountability:

- riguarda la gestione della disponibilità, l'usabilità, l'integrità e la sicurezza dei dati usati, salvati o processati in un'organizzazione,
- ha come scopo la prevenzione di un qualsiasi danno al proprietario dei dati
- può essere ottenuta mediante una combinazione di leggi, contratti, autoregolamentazioni e con l'uso di tecnologie, quali il controllo degli accessi, l'implementazione di policy e l'adozione di particolari architetture.

Un sistema distribuito gode della proprietà di *accountability* se i problemi possono essere facilmente individuati ed ognuno di essi può essere innegabilmente legato ad almeno un nodo difettoso.
Più nello specifico, il sistema deve possedere le seguenti proprietà:

- *Identities*: ogni azione è incontestabilmente legata al nodo che l'ha effettuata.
- *Secure record*: il sistema tiene traccia delle azioni compiute, così che un nodo non possa omettere, falsificare o alterare le sue voci.
- *Auditing*: le tracce possono essere ispezionate per cercare segni di guasti.

- *Evidence*: quando un'ispezione rileva un problema, può ottenere delle prove verificabili da una terza parte [47].

Nell'eventualità di un problema il cloud provider e l'utente possono utilizzare le prove per stabilire il responsabile e se non si arriva ad una soluzione si possono presentare ad una terza parte, ad esempio un giudice. Tuttavia però, le tecnologie di accountability esistenti non raggiungono ancora i requisiti richiesti dal cloud computing.

Dal momento che le piattaforme cloud sono *general-purpose*[43], il provider dovrebbe essere in grado di garantire l'accountability per qualsiasi servizio il cliente decida di eseguire. Questo esclude tecniche specifiche per alcune applicazioni come *CATS* o *Repeat and Compare*.

La tecnica indipendente dall'applicazione di PeerReview richiede modifiche al software. Il comportamento di questo, inoltre, deve essere deterministico, ma nessuna delle due situazioni è realistica nel cloud. Anche se i limiti delle soluzioni appena descritte venissero superati, potrebbero però controllare la correttezza di una sola proprietà, l'esecuzione, perché non sono progettate per controllare altre proprietà critiche per il cloud, come la protezione della confidenzialità dei dati, la disponibilità del servizio e il rispetto della SLA [47].

3.2.1 Meccanismi per implementare l'accountability nel cloud

L'accountability promuove l'implementazione di meccanismi pratici per tradurre le linee guida ed i requisiti legali in un'effettiva protezione dei dati.

Le legislazioni e le policy tendono ad essere applicate al livello dei dati, ma i meccanismi di accountability possono esistere ad ogni livello, compreso quello del sistema. È possibile progettare meccanismi legali, procedure, misure tecniche ed integrazioni tra gli stessi per supportare e sostenere questo approccio. Vediamo ora alcuni di questi meccanismi:

- I *controlli preventivi* sono costituiti, ad esempio, da una lista d'accesso che decide chi può leggere o scrivere un file o un database, oppure firewall che bloccano tutto il traffico tranne quello lecito. Questo tipo di c*ontrolli* per i sistemi distribuiti possono includere l'analisi del rischio, strumenti di supporto alle decisioni, l'applicazione delle politiche stabilite, la

[43] Di uso generale

valutazione della fiducia, le tecniche di offuscamento e la gestione dell'identità. Le organizzazioni possono utilizzare controlli per identificare i rischi sulla privacy o sulla sicurezza che vanno contro i piani e le procedure (per esempio sistemi di rilevazione delle intrusioni o strumenti di risoluzione). I controlli di investigazione per il cloud possono includere: l'auditing, il tracking, il reporting ed il monitoring.

- Sono necessari anche *controlli correttivi*, come un piano di gestione incidenti o per la risoluzione delle controversie, che possono aiutare a risolvere un effetto indesiderato che si è verificato. Queste diverse tipologie di controlli risultano essere complementari tra di loro e l'accountability richiede una loro combinazione per sussistere.
- Specialmente in un ambiente cloud, che risulta essere dinamico ed automatizzato, la *tecnologia* può svolgere un ruolo importante nel migliorare le soluzioni, applicando politiche e fornendo alle decisioni supporto, affidabilità e sicurezza.
- Le *disposizioni procedurali* includono: determinare le capacità del cloud provider, la negoziazione contrattuale, le restrizioni al trasferimento dei dati confidenziali e l'acquisto di un'assicurazione.
- Le organizzazioni dovrebbero anche nominare un *data protection officer*, eseguire regolarmente una valutazione dell'impatto sulla privacy su nuovi prodotti e servizi e mettere in atto meccanismi per consentire un rapido accesso ai dati e alla cancellazione delle richieste.
- Le *misure tecniche* per l'accountability invece includono la cifratura per la sicurezza dei contenuti ed agenti che aiutino ad aumentare la fiducia. Risulta necessario contare su infrastrutture per mantenere separazioni appropriate, per applicare le politiche e comunicare le informazioni con precisione [48].

In un ambiente cloud la già citata *intelligent accountability* comporta:

- Un allontanamento dal "*box checking*[44]" e dai meccanismi di privacy statici;

[44] Letteralmente "spuntare le caselle"

- Una valutazione dei potenziali danni prima di esporre i dati ad eventuali rischi; questo rappresenta una parte della valutazione del rischio e della mitigation, per le quali la valutazione dell'impatto sulla privacy (PIA[45]) è uno strumento importante;
- Concedere maggiore flessibilità alle organizzazioni nella protezione dei dati così da poter usare i meccanismi e i controlli interni più adatti alla loro specifica situazione aziendale, piuttosto che un set di regole uniche e prescrittive;
- L'impiego di vari gradi di accountability; standard e test più rigidi sull'accountability potrebbero facilitare alcuni CSP nel dimostrare che sono pronti o addirittura esonerarli da alcuni oneri amministrativi;
- Uno sviluppo intelligente, un'analisi automatizzata, un'applicazione automatica delle policy ed altre tecnologie per migliorare e rafforzare l'applicazione della responsabilità e evitare di aumentare il carico per gli operatori [6].

3.3 Vantaggi, problemi ed incentivi

Dal punto di vista dell'*utente* ci sono chiari vantaggi nell'adottare un sistema cloud che fa uso di accountability: primo tra tutti la possibilità di scoprire facilmente se il provider non sta eseguendo il servizio come accordato e di ritenerlo responsabile o meno.

Dal punto di vista del *provider*, però, l'accountability può rappresentare un ostacolo: potrebbe, ad esempio, far emergere problematiche che altrimenti sarebbero rimaste sconosciute, intaccando così la propria reputazione. In questo modo, parte del potere viene affidato al cliente, fornendogli le prove dell'errore.

Può risultare spontaneo chiedersi perché il cloud provider dovrebbe decidere di adottare l'accountability. Una prima ragione è sicuramente che attrae nuovi potenziali clienti. Inoltre lo stesso provider può utilizzarla per individuare e diagnosticare problemi in modo proattivo e quindi gestire più facilmente le lamentele da parte dei clienti.

[45] Acronimo di "P*rivacy Impact Assesment"*

Attualmente è difficile per i clienti distinguere tra i problemi causati dal cloud e quelli che hanno causato loro stessi, per questo motivo i provider spesso ricevono più lamentele di quelle per cui sono realmente responsabili.
Adottando l'accountability invece, il cliente ed il provider possono semplicemente eseguire un audit per determinare chi è responsabile del problema.
In alcuni scenari c'è connessione tra la privacy e l'accountability, dato che la seconda produce un registro dettagliato delle azioni delle macchine, che può essere revisionato da una terza parte. È importante però considerare cosa viene registrato e chi può vederlo. Un cloud che usa l'accountability può tenere un registro separato per ogni utente e renderlo visibile solo al legittimo proprietario. Un ipotetico cliente A quindi non potrà sapere nulla in riferimento alle azioni compiute dal cliente B, perfino la sua esistenza. La questione però rimane se l'accountability intacchi o meno la privacy del cloud provider. Visto che l'audit riporta le prove dell'errore, se queste indicano quale componente (switch, router, server, ecc) ha causato il problema, il cliente potrebbe trarre delle conclusione sulla struttura interna del cloud.
D'altra parte però queste informazioni sugli errori sono molto utili per il cloud provider, che è responsabile di diagnosticare e risolvere il problema. Per ovviare a questo problema il provider potrebbe fornire delle tracce con diversi livelli di dettaglio.
La privacy è un punto cruciale del business e presenta un rilevante problema di conformità, in quanto rappresenta un'intersezione di norme sociali, di diritti umani e di leggi. Essere conformi dal punto di vista legale e rispettare le aspettative del cliente, richiede alle organizzazioni di essere capaci di dimostrare un livello appropriato di responsabilità nel controllo sui dati, ad ogni stage dell'elaborazione, dalla raccolta alla distruzione.
La possibilità del cloud di scalare rapidamente, di archiviare dati in remoto (senza conoscere il luogo fisico) e di condividere servizi in un ambiente dinamico, può creare problemi nel mantenere un livello di privacy tale da ispirare fiducia in un potenziale cliente.

Il cloud computing presenta alcune caratteristiche che fanno sorgere specifici rischi:

- **Outsourcing**: l'esternalizzazione della computazione dei dati inevitabilmente fa sorgere domande sulla governance e sull'accountability. Chi è responsabile di assicurare che i requisiti legali sulle informazioni personali siano rispettati o che gli standard per la gestione dei dati siano applicati? Può una terza parte controllare in modo efficace il rispetto di tali leggi e norme? In che misura l'elaborazione può essere data in subappalto e come sono confermate le identità e la buona fede dei subappaltatori? O ancora quali diritti sui dati saranno acquisiti da chi elaborerà i dati e saranno trasferibili in caso di bancarotta, acquisizioni o fusioni? I modelli *on demand* e *pay-as-you-go* potrebbero essere basati su relazioni di scarsa fiducia, coinvolgere terze parti che trascurano le pratiche di sicurezza ed esporre i dati, rendendo difficile la verifica dell'effettiva cancellazione degli stessi.
- **Offshoring**: la delocalizzazione dell'elaborazione dei dati aumenta i fattori di rischio e la complessità dal punto di vista legale. Devono essere considerati i problemi di giurisdizione, di scelta della legge da applicare ed i soggetti che devono farlo. Un servizio di cloud computing che fa uso di outsourcing e offshoring può sollevare questioni molto complesse.
- **Virtualizzazione**: Possono presentarsi dei rischi di sicurezza condividendo le macchine, come la perdita di controllo sulla locazione dei dati e su chi può averne accesso. I dati delle transazioni non hanno proprietari ben definiti e può essere difficile anticipare quali potrebbero aver bisogno di protezione. Anche informazioni all'apparenza innocue potrebbero rivelarsi però sensibili per l'azienda.
- **Autonomic technology**: Concedere ad alcuni processi un certo grado di autonomia nel prendere le decisioni, per esempio per adattarsi automaticamente a nuove esigenze del cliente, spinge le aziende a mantenere gli standard di sicurezza previsti, a fornire un'adeguata continuità del servizio ma creerebbe l'impossibilità di determinare dove i dati vengono elaborati all'interno del cloud [49].

Le soluzioni per la privacy devono risolvere una combinazione di problemi, richiedono spesso nuovi meccanismi piuttosto che una combinazione di quelli già esistenti per risolvere ogni singola problematica.
Nel complesso, la velocità e la flessibilità di adattamento offerte dai provider, che apportano benefici al business e motivano l'adozione del cloud computing, portano però rischi maggiori per la privacy e per la sicurezza dei dati. Questa è una delle preoccupazioni principali, sopratutto laddove si trattano dati finanziari e sanitari.

3.4 Un esempio pratico: HP Lab

Per comprendere meglio questa tipologia di meccanismi e di processi portiamo l'esempio fornito da HP Lab[46], che ha sviluppato un sistema articolato come segue:

1. *HP Privacy Advisor* (HPPA): rappresenta un DSS[47] che supporta l'impresa responsabile, permettendo all'organizzazione di risolvere e gestire in modo corretto e proattivo gli eventuali problemi legati alla privacy. Permette di integrare la filosofia orientata al controllo responsabile con un programma ideato per educare e guidare i propri dipendenti sui requisiti della protezione dei dati, sui rischi e sulle considerazioni. Consente ai soggetti di seguire una serie di domande contestuali per valutare i rischi sui dati in riferimento ad un nuovo prodotto, servizio o programma. Questo strumento aiuta le persone a risolvere autonomamente semplici questioni e a mettersi in contatto con il responsabile della privacy per quelle più complesse e difficili.
2. *The Cloud Stewardship Economics Project:* consiste nella definizione di modelli economici e matematici nell'ecosistema cloud. L'obiettivo è quello di aiutare i consumatori, fornitori, regolatori ed altri portatori di interesse ad esplorare e prevedere le conseguenze delle diverse politiche, dei meccanismi di assicurazione e della responsabilità.

[46] La divisione di ricerca della società Hewlett-Packard (HP). Ha il compito di stabilire le strategie e le politiche di lungo termine per la società, occupandosi di ricerca avanzata per trovare applicazioni future e nuove tecnologie innovative.
[47] Decision Support System

3. Si sta inoltre lavorando per ottenere accountability anche attraverso l'adozione di *assicurazioni contrattuali* lungo l'intera catena di fornitura del servizio.

Capitolo 4: Conclusioni

In questa tesi abbiamo illustrato i concetti alla base dell'accountability, i vantaggi apportati, le attività che la supportano ed i requisiti per un approccio responsabile.
Abbiamo analizzato le principali norme sulla privacy, con particolare attenzione alla protezione dei dati personali, descrivendo le potenziali minacce e il paradigma C.I.A..
Successivamente abbiamo descritto il cloud computing soffermandoci sui quattro livelli che lo compongono e sulle tipologie di servizi offerti, che si dividono in Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). Di ciascuno sono state illustrate le tecnologie alla base e le applicazioni utilizzate per implementarli.
Infine l'accountability è stata suggerita come mezzo per raggiungere la sicurezza pratica nei sistemi distribuiti, per fornire una direttiva al comportamento cooperativo, per favorire l'innovazione e la concorrenza su Internet e per creare sistemi di rete affidabili.
La sicurezza e la gestione della privacy si evolvono nella gestione dei problemi legati alle informazioni, cioè come l'organizzazione può sorvegliare e proteggere i dati personali per conto dei proprietari, di altri soggetti o terze parti. Nel cloud computing i rischi e i doveri, le risposte operative per un'implementazione appropriata e i requisiti normativi risultano essere più difficili da stabilire rispetto ad un'architettura server tradizionale.
Rispetto a quest'ultima, nei sistemi distribuiti la trasparenza e la garanzia risultano essere aspetti più rilevanti e i controllori dei dati ed i cloud provider devono assicurare una catena di fornitura responsabile. L'accountability evidenzia la responsabilità giuridica dell'organizzazione che utilizza dati personali per assicurare che i partner a cui fornisce i dati siano conformi alle normative, ovunque essi si trovino.

Attualmente la struttura normativa pone molta enfasi sulle misure da prendere a posteriori e non induce nella giusta misura le organizzazioni a ridurre proattivamente i rischi legati alla privacy e alla sicurezza. I nuovi modelli di governance dei dati possono fornire delle basi per la protezione nel cloud.

Il rafforzamento di un approccio di responsabilità e lo sviluppo di una metodologia intelligente per applicare l'accountability alla gestione delle informazioni è una sfida continua, che va oltre il tradizionale approccio alla protezione dei dati.

Un corretto utilizzo dei meccanismi di accountability contribuisce quindi ad aumentare la fiducia degli utenti nei confronti dei sistemi cloud, ad oggi percepiti come rischiosi rispetto ai sistemi tradizionali, garantendone così una maggiore diffusione.

Bibliografia

[1] D. Catteddu and G. Hogben, “Cloud Computing: Benefits, Risks and Recommendations for Information Security”, ENISA, Nov. 2009.

[2] Top Threats to Cloud Computing, version 1.0, tech. Report, Cloud Security Alliance, Mar 2010.

[3] Organization for Economic Cooperation and Development (OECD), “Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data”, 1980

[4] Galway Project, “Galway Project Plenary Session Introduction”, 28 Apr. 2009, p.5.

[5] Vaquero L, Rodero-Merino L, Caceres J, Lindner M (2009) A break in the clouds: towards a cloud definition. ACM SIGCOMM computer communications review

[6] Siani Pearson, Toward Accountability in the Cloud, IEEE, Internet Computing, 30 Jun 2011, pp. 64-69

[7] Michael Armbrust e altri - Above the clouds: A Berkeley View of cloud computing, Electrical Engineering and Computer Sciences, University of California, Berkeley (CA), 10 Febbraio 2009

[8] ISCOM - L'analisi e la gestione del rischio: principi e metodi, Novembre 2005 http://www.isacaroma.it/html/newsletter/node/118

[9] Lorenza Rusca, “Informatica e protezione dei dati”, Marzo 2003 http://www4.ti.ch/fileadmin/CAN/ICPD/PDF/TEMI/2003-4-p17.pdf

[10] Dykstra, Clarence A. (February 1939). "The Quest for Responsibility". American Political Science Review (The American Political Science Review, Vol. 33, No. 1) 33 (1): 1–25

[11] Williams, Christopher (2006) Leadership accountability in a globalizing world. London: Palgrave Macmillan

[12] Abrams, Martin (2009) Data Protection Accountability: The Essential Elements. A Document for Discussion. Accountability: A Compendium for Stakeholders, pp. 8-9, 11-14

[13] Onora O’Neil, “A Question of Trust”, BBC Reith Lectures, 2002, www.bbc.co.uk/radio4/reith2002/

[14] A. Yumerefendi and J. Chase, “Strong Accountability for Network Storage”, ACM Transactions on Storage (TOS), 2007, 3(3)
http://www.cs.duke.edu/nicl/pub/papers/cats-fast07.pdf
[15] Gerome Miklau, Brian Neil Levine, Patrick Stahlberg, “Securing history: Privacy and accountability in database systems”, In Proceedings of CIDR, 2007, pp.387-396 , http://www.cidrdb.org/cidr2007/papers/cidr07p44.pdf
[16] Andreas Haeberlen, Petr Kuznetsov, and Peter Druschel, “PeerReview: Practical accountability for distributed systems”, In Proc. SOSP, October 2007.
http://www.cis.upenn.edu/~ahae/papers/peerreview-sosp07.pdf
[17] N. Michalakis, R. Soulè, and R. Grimm., “Ensuring content integrity for untrusted peer-to-peer content distribution networks”, In Proc. NSDI, Apr 2007, http://cs.nyu.edu/rgrimm/papers/nsdi07.pdf
[18] Qi Zhang, Lu Cheng and R. Boutaba, “Cloud computing: state-of-the-art and research challenges”, Journal of Internet Services and Applications, Vol. 1, No. 1, April 2010, pp. 7-18
[19] J. Broberg, “Introduction to Cloud Computing”, University of Melbourne, 2009
[20] John Bruschi, Peter Rumsey, Robin Anliker, Larry Chu, and Stuart Gregson, “Best Practices Guide for Energy-Efficient Data Center Design”, Rumsey Engineer - National Renewable Energy Laboratory, Marzo 2011.
[21] http://www.google.com/about/datacenters/locations/hamina/ Hamina Data Center, Google.
[22] Bo Li, Jianxin Li, Jinpeng Huai, Tianyu Wo, Qin Li, Liang Zhong, “EnaCloud: An Energy-saving Application Live Placement Approach for Cloud Compunting Environments”, IEEE International Conference on Cloud Computing, 2009
[23] PDUs Direct, http://pdusdirect.com/
[24] Mission Critical Modular Data Center Solution Selected by Pelio & Associates to Meet Tenants' Power, Energy Efficiency, Scalability and JIT Requirements, http://www.marketwire.com/press-release/pdis-i-con-tapped-for-1101-space-park-modular-data-center-1392990.htm
[25] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. "The Google File System", Google, 2006.
[26] Hadoop Distributed File System, http://hadoop.apache.org/hdfs/

[27] Wallach Mike Burrows, Tushar Chandra, Andrew Fikes, Robert E. Gruber. "Bigtable: A Distributed Storage System for Structured Data", Google, 2006

[28] Kannan Muthukkaruppan, "The Underlying Technology of Messages", Nov. 2010, https://www.facebook.com/note.php?note_id=454991608919

[29] Jeremy Reimer, "Amazon reveals its distributed storage 'Dynamo'", Oct. 2007 http://arstechnica.com/old/content/2007/10/amazon-reveals-its-distributed-storage-dynamo.ars

[30] Cassandra Wiki, http://wiki.apache.org/cassandra/

[31] Je_rey Dean, Sanjay Ghemawat - MapReduce: simpli_ed data processing on large clusters, 6th Symposium on Operating System Design and Implementation (OSDI'04), San Francisco (CA), 5 Dicembre 2004

[32] Amazon Elastic MapReduce (Amazon EMR), http://aws.amazon.com/elasticmapreduce/

[33] Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/

[34] Flexiscale, http://www.flexiscale.com/

[35] GoGrid, http://www.gogrid.com/cloud-hosting/

[36] Daniel Nurmi et al, "The Eucalyptus Open-source cloud-computing System", 9th IEEE/ACM International Symposium on Cluster computing and the Grid at IEEE Computer Society (CCGRID'09), Washington (WA), 18-21 Maggio 2009,Vol. 0, pp. 124-131

[37] Openstack, http://openstack.org/

[38] Google App Engine, http://code.google.com/appengine/docs/

[39] Windows Azure, http://www.windowsazure.com/en-us/home/features/overview/

[40] Amazon Web Services, Application Hosting, http://aws.amazon.com/application-hosting/

[41] Force.com for Google App engine, http://developer.force.com/appengine

[42] Cloud Taxonomy, http://cloudtaxonomy.opencrowd.com/taxonomy/software-as-a-service/

[43] Google Apps, http://www.google.com/apps/intl/en/group/index.html

[44] http://www.force.com/why-force.jsp

[45] Fujitsu Research Institute, "Personal data in the cloud: A global survey of consumer attitudes," 2010,

http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf

[46] Alan Le Marquand, “Windows Azure Platform. Inside the Cloud. Microsoft's Cloud World Explained Part 2.”, May 2010, http://technet.microsoft.com/en-us/edge/ff945094

[47] Andreas Haeberlen, “A Case for the Accountable Cloud”, 2009

[48] A. Baldwin and S. Shiu, Managing Digital Risk: Trends, Issues, and Implications for Business, tech. report, Lloyds 360 Risk Insight, 2010

[49] Siani Pearson and Andrew Charlesworth, “Accountability as a Way Forward for Privacy Protection in the Cloud”, 2009

[50] London Institute of InfoTech and Professional Training (LIIPT), licit.com

[51] Every company needs to have a security program, http://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program