

Il Cloud, un'opportunità per il futuro: Pro e Contro

Vincenzo Ciminelli



Ingegnere
Informatico, UOC
Servizio
Informativo
Aziendale ASP
Cosenza

autore

Michelina Graziano

Fisico Medico, UOC
Radiodiagnostica ASP
Cosenza, Membro GdL RIS-
PACS Associazione Italiana
di Fisica Medica (AIFM)



autore

INTERACTIVE NEWS

In uno scenario in cui tagli alla spesa sanitaria e incrementi sui ticket sembrano le scelte più facili per risanare il debito nazionale, l'economia mondiale va a rotoli e l'Italia si classifica al quarto posto nell'area dell'euro per pressione fiscale, l'unico mercato che sembra essere inarrestabile è quello delle nuove tecnologie. Il mercato tecnologico si rinnova con una velocità tale che nemmeno le grandi società scientifiche riescono a stare al passo e così si finisce col perdere di vista il fine primo e ultimo dell'opera di chi pratica in ambito sanitario: il paziente e il suo bene. Ormai si lavora con i numeri e per i numeri. Efficacia, efficienza ed economicità sono solo parametri per fatturare, perché il paziente non è più il soggetto da curare e guarire, ma è un numero incrementale che permette di fare budget. Una triste conclusione, soprattutto perché dietro all'interesse del medico per l'innovazione tecnologica si cela troppo spesso il desiderio narcisista di voler dimostrare di essere più "accessoriati" degli altri e così si finisce con lo sperperare il danaro pubblico. Ultima frontiera, nell'ambito dell'informatica sanitaria, è rappresentata dal *cloud computing*, una nuvola di super tecnologia informatica, dietro il cui business si celano problemi di sicurezza e privacy non indifferenti. Scopo di questo lavoro è spiegare come nasce un cloud, come funziona e, senza fare terrorismo mediatico, spiegare i pro e i contro di questa tecnologia, che, come vedremo, è penetrata così tanto nel tessuto sociale da modificare le nostre abitudini.

Nell'ambito dell'informatica sanitaria, l'ultima frontiera è rappresentata dal cloud computing, dietro il cui business si celano problemi di sicurezza e privacy non indifferenti. Da qui la necessità di porsi (e porre) una serie di interrogativi: come nasce e come funziona un cloud? Quali sono gli aspetti positivi e quelli negativi di questa tecnologia?

MATERIALI E METODI

Noi percepiamo il mondo che ci circonda attraverso i nostri sensi, i quali traducono degli stimoli esterni in sensazioni interne al nostro corpo. Tutto quello che percepiamo e che possiamo trasmettere verso il mondo esterno contiene delle informazioni. Il concetto di informazione è fondamentale nella vita degli esseri umani, e fondamentale per la vita stessa della nostra società è la possibilità di scambiarsi informazioni. Conversare, guardare un film in televisione, navigare su Internet, utilizzare un social network, telefonare, inviare e ricevere sms, mms, sono tutti modi che oggi abbiamo per scambiarsi informazioni. Ogni scambio di informazioni presuppone la possibilità di avere un mezzo per trasferire le stesse da una sorgente ad una destinazione: il mezzo trasmissivo.

Esistono vari mezzi trasmissivi, ma quello che oggi consente di trasferire la maggior quantità di informazioni in assoluto è Internet, e in generale le reti di trasmissione dati. È molto difficile definire quant'è grande Internet, ma possiamo riflettere su alcuni ordini di grandezza:

- 2,4 miliardi di utenti nel mondo usano Internet;
- 144 miliardi di email al giorno circolano su Internet;
- 700 milioni di pagine web sono raggiungibili e consultabili su Internet;
- 246 milioni di domini esistono su Internet;
- 1 miliardo di utenti sono registrati su Facebook, postano ogni mese 7 petta-

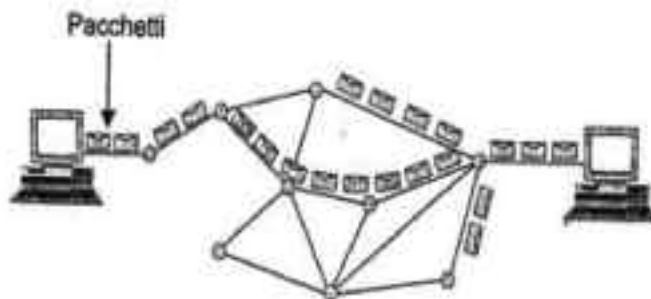
byte di immagini, circa 300 milioni di foto al giorno;

- 1,2 trilioni di ricerche effettuate su Google solo nel 2012.

Insomma ad Internet corrispondono numeri da capogiro, che corrispondono ad informazioni che transitano sulle reti di trasmissione dati e sono di tipo digitale. Ma era proprio necessaria la "rivoluzione digitale"? L'*Information Technology IT* ha rappresentato una rivoluzione perché i segnali digitali sono facilmente memorizzabili, rielaborabili e trasmissibili, garantendo al contempo la loro conservazione nel tempo e nello spazio, a differenza dei segnali di tipo analogico, la cui gestione comportava enormi dispendi di energia, di spazio, con poche garanzie sull'integrità delle informazioni. Mentre un segnale analogico è molto sensibile ai disturbi del mezzo trasmissivo, subendo di per sé un'attenuazione causata dalle caratteristiche fisiche del mezzo stesso, i segnali digitali sono perfettamente rigenerabili senza perdita alcuna, malgrado il perdurare delle attenuazioni in fase trasmissiva. Per trasmettere questo universo di informazioni attraverso le reti dati, Internet compresa, si utilizza una tecnica trasmissiva detta **commutazione di pacchetto**.

In realtà le lunghe sequenze di bit che compongono ad esempio una foto che si desidera postare su Facebook, devono essere scomposte in gruppi, inglobate in oggetti detti **pacchetti** rappresentabili come buste per lettere, e quindi inviate sulla rete. Ad oggi questo meccanismo è la base del funzionamento di tutte le reti informatiche, Internet compresa, ed il suo funzionamento è regolato fondamentalmente dalla coppia di **protocolli di comunicazione** detti TCP/IP (Transmission Control Protocol/Internet Protocol). Internet viene raffigurata come una **nuvola** nella quale possiamo immaginare l'esistenza di un universo digitale, ed oggi questa immagine viene sempre di più utilizzata per rappresentare un fenomeno in rapida evoluzione chiamato **Cloud Computing**. In letteratura scientifica il *cloud computing* ha diverse definizioni, ma in sostanza è una nuova metodologia utilizzabile per fornire risorse IT (capacità computazionale, spazio di memorizzazione o anche software) sotto forma di servizi accessibili via rete. Esistono varie definizioni di cloud. Il **National Institute of Standards and Technology (NIST)**, ad esempio, definisce il *cloud computing* "un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio rete, server, dispositivi di memorizzazione, applicazioni e servizi) sotto

Il cloud computing, anche se probabilmente non appare evidente, è ormai parte integrante del mondo digitale moderno



forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore".

Per il NIST il cloud deve avere cinque caratteristiche fondamentali:

- **On-demand self-service:** un cliente può unilateralmente richiedere nei vincoli fissati dal contratto risorse computazionali, come tempo macchina, risorse di memorizzazione o altro, quando necessario per svolgere i suoi task, senza richiedere un intervento umano dei fornitori dei servizi stessi;
- **Broad network access:** tutte le funzionalità del cloud sono accessibili attraverso la rete, la cui banda deve essere adeguata all'uso specifico richiesto, e sono fruibili tramite standard che agevolano l'utilizzo di terminali e piattaforme eterogenei;
- **Resource pooling:** le risorse di calcolo del fornitore vengono organizzate per servire più clienti, utilizzando il modello *multi-tenant*, in cui le risorse fisiche e virtuali sono assegnate dinamicamente e de-allocate ai *consumer* in relazione alla richiesta dei clienti. Le risorse offerte sono indipendenti dalla loro locazione fisica, ovvero il cliente generalmente non ha né il controllo né la conoscenza dell'esatta locazione fisica delle risorse a lui fornite. Tuttavia, il fornitore potrebbe permettere all'utente di specificare dei vincoli sulla locazione delle risorse a lui assegnate in termini di area geografica, Paese o anche singolo *data center*. Esempi di risorse sono: risorse di memorizzazione, di calcolo, di rete e macchine virtuali;
- **Rapid elasticity:** le risorse possono essere fornite rapidamente ed elasticamente – e in alcuni casi anche automaticamente – per incrementare velocemente la capacità computazionale; allo stesso modo possono essere rapidamente rilasciate per decrementare la capacità computazionale e per renderle disponibili ad altri potenziali utilizzatori;
- **Measured Service:** i sistemi cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse, sfruttando la capacità di misurarne l'utilizzo delle risorse al livello necessario per il tipo di servizio. Questa tecnologia può fornire tre modelli di servizi (*IaaS*, *PaaS*, *SaaS*) e quattro modelli di gestione dei *data center* (Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud):
- Il modello **IaaS**, *Infrastructure as a Service*, prevede che il servizio offerto consista in una infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale l'utente possa installare ed eseguire il software a lui necessario, dal sistema operativo alle applicazioni;
- Il modello **PaaS**, *Platform as a Service*, prevede che il fornitore del servizio metta a disposizione dell'utente una interfaccia di programmazione (API) con la quale l'utente può scrivere applicazioni che interagiscono con il servizio;
- Il modello **SaaS**, *Software as a Service*, prevede che il servizio offerto sia un'applicazione software che può essere utilizzata su richiesta;
- Il **Public Cloud:** in cui il fornitore mette a disposizione dei suoi clienti/utenti i suoi servizi cloud pubblici, secondo politiche, modelli, prezzi stabiliti unilateralmente dal fornitore stesso. L'infrastruttura è sempre gestita dalla società provider;

- Il **Private Cloud:** in cui l'utente/cliente utilizza il proprio *data center* per il proprio cloud privato. In questo caso le politiche di gestione e i modelli di cloud sono determinati dal cliente/utente stesso. Il *private cloud* può anche essere implementato presso un *data center* offerto da un soggetto terzo;
- Il **Community Cloud:** in cui l'infrastruttura presso la quale sono installati i servizi cloud è condivisa da un insieme di soggetti, con esigenze comuni. L'infrastruttura può essere gestita dalla comunità stessa oppure da un fornitore terzo;
- L'**Hybrid Cloud:** è una combinazione del *Private* e del *Public Cloud*. Si tratta di una soluzione che validamente potrebbe risolvere il problema del trattamento dei dati sensibili, gestendoli nel cloud privato, e al contempo consente di avere sistemi di *backup* e *disaster recovery*, oppure computazioni che non coinvolgono dati sensibili gestendoli nel cloud pubblico.

Da una ricerca condotta dalla IDC (International Data Corporation) nel 2012 la spesa in servizi cloud pubblici e privati, e gli investimenti necessari per la costruzione di questi, risulta abbiano portato il mercato cloud a valere 60 miliardi di dollari a livello mondiale, mentre in Italia una azienda su quattro ha già adottato una o più tipologie di servizi IT Cloud: il 17,2% ha adottato servizi a livello applicativo, il 16% a livello infrastrutturale e il 9% di piattaforma. Sempre secondo IDC, nel 2015 la spesa in servizi erogati tramite cloud pubblica raggiungerà i 72,9 miliardi di dollari a livello mondiale con una crescita importante che coinvolgerà anche il nostro Paese: le previsioni di IDC proiettano il mercato dei servizi di public cloud in Italia verso la soglia dei 900 milioni di euro. Da questi dati, presentati al *Cloud Symposium* tenutosi a Milano lo scorso marzo, emerge come le aziende siano molto concentrate ad approcciare questo nuovo modello e, secondo i dati dell'IDC, con una priorità nei confronti dei servizi



Software as a Service (SaaS) e Platform as a Service (PaaS). Il risultato di questo business, secondo IDC, è che oltre l'80% delle nuove applicazioni sarà erogato via cloud!

La specifica natura del **cloud computing** comporta:

1. che le informazioni aziendali siano trattate in contesti esterni al perimetro dell'organizzazione e potenzialmente condivisi con gli altri clienti del *cloud provider*;
2. l'utilizzo strutturale di reti pubbliche per connettere l'ambito aziendale con il cloud;
3. l'accessibilità delle informazioni aziendali senza vincoli di orario e di luogo da parte degli utenti.

Ciò implica che, oltre a gestire gli aspetti strettamente tecnologici, l'adozione di soluzioni cloud impatta su molti processi aziendali, tra i quali quelli di *governance*,

di gestione delle identità e degli accessi, fino alle attività di controllo e di *audit*, che non devono essere condizionate nella loro efficacia dal nuovo paradigma. Il Garante della Privacy – nell'ottica di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici tramite cloud pubbliche, che comportano l'esternalizzazione di dati e documenti – invita le aziende alla garanzia della tutela dell'importante patrimonio informativo costituito dai dati personali e particolarmente sensibili gestiti su questi sistemi.

DISCUSSIONE

Il *cloud computing*, anche se probabilmente non appare evidente, perché trasparente per l'utente finale, è ormai parte integrante del mondo digitale moderno, costituendo in effetti la grossa parte delle infrastrutture tecnologiche su cui sono basati i servizi utilizzabili su Internet, come i servizi di posta elettronica gratuiti o a pagamento, i motori di ricerca, i social network, i blog, i siti web. Di conseguenza non si ha neppure la consapevolezza dei possibili rischi nei quali incorrono le informazioni che si trasferiscono attraverso questi servizi oggi di uso comune.

Inoltre, poiché i dati gestiti nella nuvola di Internet sono maggiormente dati sensibili, ciò fa sì che il fornitore di un servizio in cloud non è solo un *cloud provider* di tecnologia avanzata, ma, ai sensi dell'art.

29 del Codice della Privacy, egli è **Responsabile dei trattamenti dei dati** a lui affidati ed è garante dell'efficacia delle misure adottate per la protezione degli stessi. Cosa ben diversa è invece la titolarità dell'azienda cliente in merito a tutte le responsabilità che gli sono attribuite dalla legge nei confronti degli interessati, cioè dei proprietari dei dati personali. Le responsabilità dell'azienda titolare dei dati, in quanto produce e utilizza le informazioni prodotte, riguardano non solo la sicurezza dei dati personali ma anche la tutela dei diritti che rimangono in capo all'interessato relativamente al consenso ed alla sua revoca, alla modifica dei dati, etc.

A complicare gli aspetti relativi alla sicurezza delle informazioni circolanti sulla nuvola contribuisce in modo non trascurabile la stessa architettura funzionale su cui si basa Internet.

Già dal momento in cui un utente inizia a trasmettere le sue informazioni sulla rete, egli perde ogni controllo sul percorso che le stesse seguiranno per giungere a destinazione. Questo è spiegabile richiamando il concetto sopra descritto della **trasmissione a commutazione di pacchetto**. In realtà una sessione trasmissiva su Internet può percorrere segmenti di reti non note a priori e, al limite, ogni singolo pacchetto della sessione potrebbe percorrere segmenti di rete completamente diversi da tutti gli altri pacchetti, prima di essere riassemblati al raggiungimento della loro destinazione. Questo scenario implica che la sicurezza delle informazioni trattate sul cloud, e su Internet in generale, non dipende solo da come vengono implementate e gestite le politiche di information security lato cliente e lato *cloud provider*, ma dipendono anche da tutte le politiche di sicurezza implementate dai vari provider di connettività gestori delle reti che costituiscono Internet.

Poiché la normativa sulla privacy dedica una particolare attenzione alla esportazione dei dati verso contesti regolati da normative diverse, è necessario riservare una particolare attenzione a questi aspetti.

Un ultimo aspetto rilevante, sotto il profilo legale, riguarda la possibilità che il *cloud provider* si avvalga, nell'erogazione del servizio offerto, dei servizi cloud di altri provider (ad es. un provider SaaS potrà utilizzare l'infrastruttura di un provider IaaS), dando vita a una cosiddetta catena di cloud. È evidente come tali configurazioni aumentino la flessibilità e l'efficienza dell'offerta, ma comportino rischi aggiuntivi per l'azienda che dovranno essere opportunamente indirizzati in sede contrattuale, in particolare garantendo la piena responsabilizzazione dell'intera catena. La normativa impone l'adozione di misure minime di sicurezza alle quali il provider di *cloud computing* deve essere vincolato contrattualmente, anche in considerazione delle implicazioni penali di una loro violazione.

CONCLUSIONI

Il *cloud computing* ha portato non solo al risparmio e alla razionalizzazione nei *data center* aziendali, ma ha permesso di realizzare infrastrutture condivise che facilitano drasticamente la progettazione, la realizzazione e la gestione dei sistemi informativi. I servizi cloud si presentano come uno dei mezzi più economici per assicurare alle aziende quelle caratteristiche di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza previ-

ste dal Codice dell'Amministrazione Digitale. Il *cloud computing* rappresenta un nuovo paradigma per i servizi di Information and Communication Technology che consente alle aziende di usufruire di maggior flessibilità e scalabilità dei servizi, permettendo loro di concentrarsi sul proprio *core business* grazie ad una riduzione dei costi complessivi di gestione dell'informatica. Proprio in virtù di tali potenziali benefici per le aziende, si è assistito negli ultimi due anni a un progressivo incremento, in numerosità e complessità, sia delle tipologie di servizi fruibili dal *cloud* sia delle tipologie di fornitori di servizi cloud che ha dato vita ad un ecosistema d'offerta particolarmente articolato e complesso. Di contro la Pubblica Amministrazione si trova di fronte a complesse problematiche economiche, finanziarie, tecnologiche, giuridiche, contrattuali, organizzative e amministrative, per cui l'adozione di queste soluzioni innovative comporta notevoli sforzi economici ed organizzativi, che ad oggi la stessa non sempre è pronta ad affrontare.

A ciò si affianca il timore di adeguarsi a nuovi sistemi di gestione informatizzata di dati sensibili su larga scala, con conseguenti rischi di natura legale, derivanti dalla possibilità per i fornitori di servizi cloud di disporre di infrastrutture in vari luoghi geografici, il che espone il cliente a diverse giurisdizioni e dunque a complesse gestioni di eventuali contenziosi.

Da una ricerca condotta dalla International Data Corporation, in Italia una azienda su quattro ha già adottato una o più tipologie di servizi IT Cloud

Dalla particolare prospettiva della privacy ciò significa che, in molti casi, tali giurisdizioni possono non essere coerenti con la normativa di protezione dei dati del Paese di provenienza, rendendone difficile l'applicazione e creando possibili contenziosi di natura legale. Sarebbe auspicabile che le aziende, prima di adottare qualunque scelta strategica tesa all'esternalizzazione dei servizi e prima di investire in qualsiasi innovazione tecnologica, investissero nello sviluppo del *know-how* delle proprie risorse umane, specialmente nell'ambito delle tecnologie emergenti. Questa impostazione permetterebbe alle aziende di pianificare e realizzare progetti perfettamente ritagliati sui propri bisogni reali, di assumersi pienamente la responsabilità delle proprie scelte strategiche, con il massimo soddisfacimento della propria utenza. ■

BIBLIOGRAFIA

1. Fondazione Astrid e Fondazione Res Pubblica, L'impatto del cloud computing sull'economia italiana, novembre 2011;
2. D. Catteddu e G. Hogben, Cloud Computing: Benefits, Risks and Recommendations for Information Security, 2009 European Network and Information Security Agency (ENISA);
3. Relazione annuale sullo stato dell'ICT nella PAC, 2008 CNIPA;
4. Matteo Cavallini, Cloud security: una sfida per il futuro, II/2011 Quaderni CON-SIP;
5. Cloud Computing: indicazioni per l'uti-



lizzo consapevole dei servizi, Garante per la protezione dei dati personali, 2010;

6. Cloud computing e tutela dei dati personali in Italia: una sfida d'esempio per l'Europa, settembre 2011 Istituto Italiano per la Privacy in "Diritto, Economia e Tecnologie della Privacy";
7. P. Mell, T. Grance, The NIST Definition of Cloud Computing. Recommendation of the National Institute of Standards and Technology (NIST), January 2011 U.S. Department of Commerce;
8. NIST Cloud Computing Reference Architecture, September 2011;
9. Cloud Computing Standards Roadmap, July 2011 NIST;
10. DRAFT Cloud Computing Synopsis and Recommendations, May 2011 NIST;
11. J. Reavis e D. Catteddu, Cloud Security Alliance Contribution to the European Commission Strategy on Cloud Computing, November 2011;
12. Alessandro Mantelero, Law and Policy of the Media in a Comparative Perspective Cloud Computing. Legal aspects, 2011 Articles from MediaLaws;
13. Caterina Flick e Vincenzo Ambriola, Dati nelle nuvole: aspetti giuridici del Cloud Computing e applicazione alle Amministrazioni Pubbliche, Federalismi.it 6/2013.

NORMATIVA

1. D. Lgs. 82/2005 - Codice dell'Amministrazione Digitale;
2. Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione, 2006 CNIPA;
3. Linee guida per il disaster recovery delle pubbliche amministrazioni, 2011 DigitPA;
4. Raccomandazioni e proposte sull'utilizzo del Cloud Computing nella Pubblica Amministrazione, 2012 DigitPA.

Oltre a gestire gli aspetti strettamente tecnologici, l'adozione di soluzioni cloud impatta su molti processi aziendali