Cloud Computing

Benefici, criticità ed aspetti di interesse per l'Informatica forense

Computer Forensics
Università di Catania
Catania, 15 aprile 2013

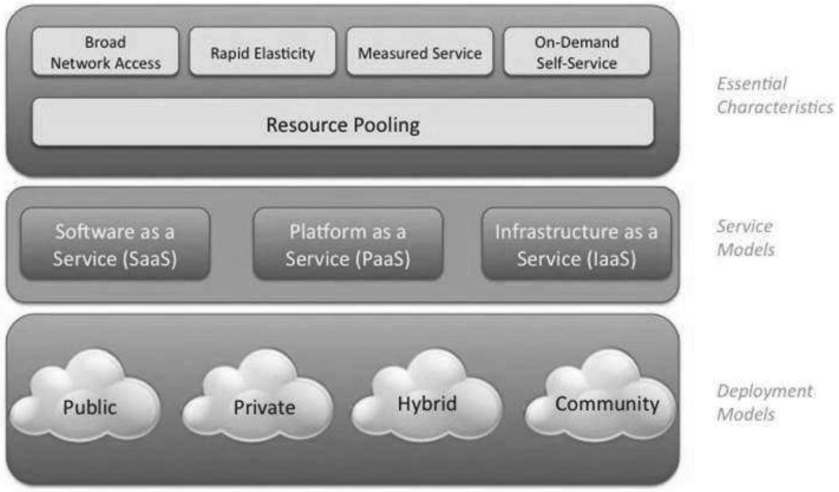
Indice

- Principi di base del Cloud Computing
- Opportunità e criticità del Cloud Computing
- Il Cloud Computing per l'Informatica forense

Cos'è

- ICT come servizio
  - Si paga a consumo, come l'acqua, l'elettrica e il gas
- Disponibilità di servizi ICT a buon mercato erogati tramite rete
  - Scalabili dinamicamente
  - Tariffati sul reale utilizzo
- Punti di riferimento geografici blandi rispetto al tradizionale hosting

Definizione formale del Cloud Computing NIST



Modelli di servizio: SaaS

- L'utente finale affitta una piattaforma software preconfezionata con applicazioni di vario tipo
  - Produttività di ufficio, CRM, vendite…
- SaaS consente ad un'organizzazione che ne fa uso di concentrarsi solo sul proprio core business
  - Nessuna preoccupazione della gestione tecnica dell'infrastruttura
  - Responsabilità solo per la scelta iniziale del prodotto
  - Nessun controllo su formato di dati e tecniche di protezione

Modelli di servizio: PaaS

- Gli utenti possono sviluppare applicazioni da zero con linguaggi di programmazione di alto livello (Java, C#...) che utilizzano le risorse hardware sottostanti
  - Interfaccia applicativa (API) esposta dal fornitore del servizio
  - Il cliente è responsabile dei difetti del software
    - Ad esempio, errori di scrittura del codice o di configurazione
  - Nessun carico derivante dalla gestione del sistema informatico

Modelli di servizio: IaaS

- Data center virtuale a disposizione dell'utente che ha delle credenziali per amministrare le macchine virtuali
  - Ampia libertà nella scelta dei sistemi operativi, tecnologie di base e linguaggi di programmazione
  - Gestione logica del sistema informativo
  - Responsabilità del cliente nella gestione del sistema informatico
  - Il fornitore del servizio è responsabile della sicurezza fisica

I CSP più noti


I CSP made in Italy

Un confronto tra CSP

	Tipologia	Costo piattaforma	Traffico di rete
amazon web services	1 server large instance: •7.5 GB RAM •4 CPU virtuali •Piattaforma Win 64bit	0,46 $/h (0,24 $/h per istanze spot)	IN: •gratuito OUT: •gratuito fino a 1 GB/mese •0,12$/GB fino a 10 TB/mese •Prezzi inferiori a crescere
aruba CLOUD.it COMPUTING	1 server: •8 GB RAM •4 CPU virtuali •850 GB spazio	0,37 €/h (+ IVA)	illimitato

Qual è la novità?

- Il Cloud è basato su tecnologie consolidate
  - Virtualizzazione, Disaster recovery, outsourcing…
- Risolve problemi noti
  - Continuità del business
  - Bassa utilizzazione media dei sistemi
  - Picchi della domanda non gestiti
  - Lunghi tempi di acquisizione di beni e servizi
  - Disponibilità immediata
  - Costi di esercizio rispetto a immobilizzazioni

Fattori chiave

- Estrema ristrutturazione della gestione dei data center
- Economie di scala nell'acquisto di materiali e servizi
- Uso di commodity hardware (COTS)
- Minore disponibilità economica per allestire un data center
  - Fine dei data server sotto utilizzati?
- Applicazioni software su cloud invece che in rete locale

Benefici

- Partenza facile
  - Chi comincia un business non ha impegni a lungo termine, nè elevati costi iniziali
- Piattaforma IT elastica
  - Le risorse computazionali possono crescere per far fronte a picchi di domanda, possono decrescere nei tempi morti
  - Le risorse di storage possono crescere per far fronte a picchi di domanda, possono decrescere nei tempi morti
- Nessun problema di approvigionamento e di spazi
  - Non c'è hardware che costituisce un data server
  - Si comprano servizi,non asset

Opportunità

- Ottimo per
  - Nuove aziende
  - Test di progetti
  - Esigenze di durata nota
    - Ad esempio, campagne elettorali/elezioni
  - Elaborazioni caratterizzate da picchi di utilizzo
    - Picchi noti
    - Picchi incogniti

Criticità

- Perdita di controllo
  - Riservatezza e disponibilità dei dati
- Rispetto delle norme
- Rispetto delle politiche dichiarate dal CSP
  - Wiping?
  - Localizzazione geografica dei dati?

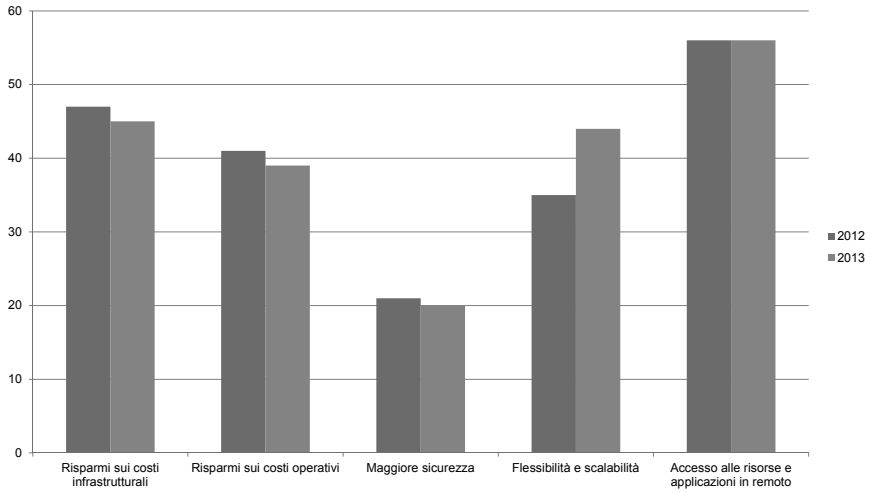
Aspetti preoccupanti

- Sicurezza
  - Questioni di sicurezza fisica e/o logica
  - Intrusioni dall'esterno, ma anche dall'interno
- Concentrazione di valore
  - Piattaforme dei CSP appetibili dai cybercriminali
- Lock-in
  - Formato di dati del proprietario e modalità di migrazione verso altro fornitore

Gestione del rischio

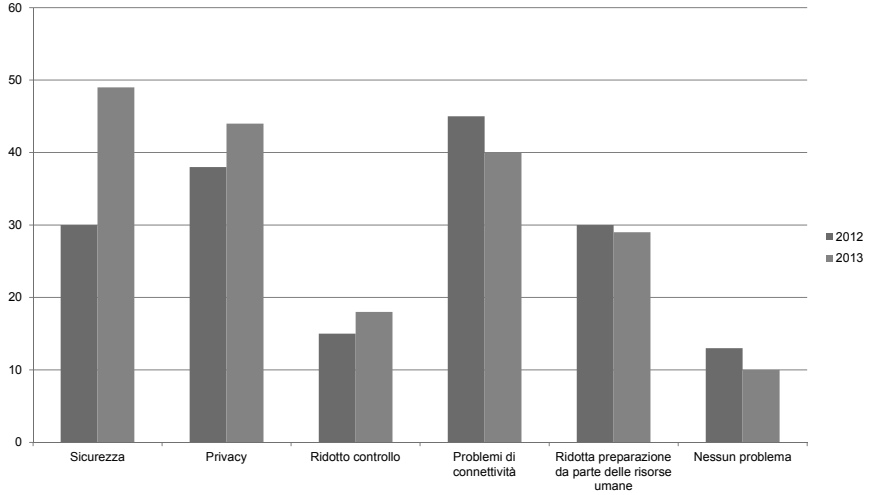
- Migrare verso il cloud non è un problema tecnico ma di risk management
  - Bilanciare benefici e rischi
  - Comprendere e ridurre i rischi
  - Evitare di inseguie aspettative irrealistiche

Cloud Survey: benefici percepiti (2012 – 2013)



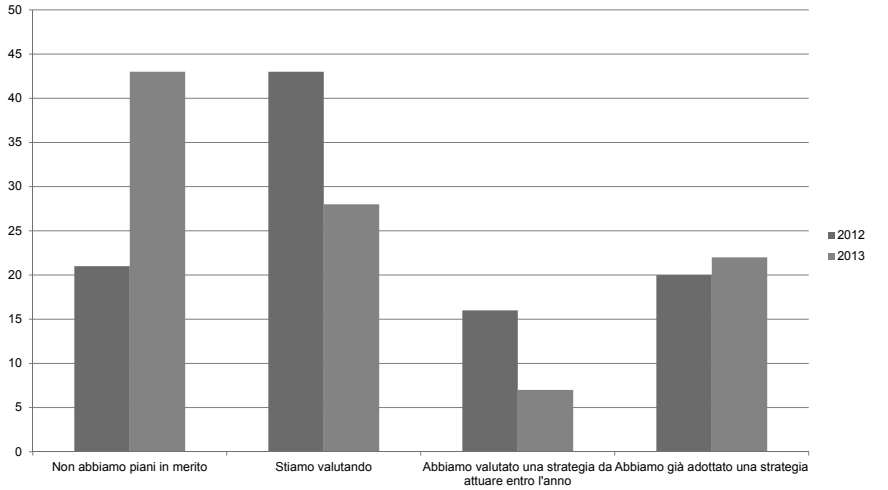
Fonte dei dati: www.enterthecloud.it

Cloud Survey: fattori frenanti (2012 – 2013)



Fonte dei dati: www.enterthecloud.it

Cloud Survey: prospettive (2012 – 2013)



www.enterthecloud.it

Cloud computing per il Garante

- L'autorità Garante della Privacy Italiana ha pubblicato una guida all'uso "consapevole" dei servizi di Cloud
- Delegare a terzi la gestione dell'IT non toglie ad aziende e PA le responsabilità derivanti dalle norme sulla protezione dei dati personali
  - Valutare il rapporto rischi/benefici
    - Cosa succede se i dati vengono disvelati, cancellati o non sono in linea?
  - Verificare l'affidabilità del fornitore
    - Referenze, policy di sicurezza e di business continuity, certificazioni…
  - Privilegiare CSP che garantiscono la portabilità dei dati
  - Assicurarsi copie locali dei dati per emergenza
  - Informarsi sulla locazione geografica reale dei dati
  - Responsabilità del CSP, protezione dei dati, politiche di porting e takeback

L'IF ai tempi del cloud computing

L'informatica forense ai tempi del cloud computing

Criticità nel cloud computing per l'IF

- Un accesso diretto ai dispositivi tramite sequestro o acquisizione bit stream potrebbe rivelarsi un incubo presso i locali del CSP senza incidere sul suo business
  - Le applicazioni Cloud devono scalare rimanendo però reattive e tolleranti a guasti/disastri
  - I servizi Cloud devono inoltre costare poco e questo richiede l'utilizzo di COTS

Criticità nel cloud computing per l'IF

- Tutto questo è ottenuto distribuendo frammenti di dati su diversi elaboratori, potenzialmente anche geograficamente distanti
- Difficoltà di ricostruzione dello scenario distribuito
- Soluzioni non rigorose abbasserebbe il livello di qualità dell'accertamento
  - Limiti sull'ammissibilità e l'utilità in dibattimento

Criticità nel cloud computing per l'IF

Criticità nel cloud computing per l'IF

- CSP clienti di CSP
  - Esempio: Dropbox si appoggia ad Amazon S3
- Necessità di rivolgersi a CSP diverse
- Considerate per esempio il caso di un provider belga che produce una suite per la produttività d'ufficio, ma usa macchine virtuali e spazio di backup affittate da società francesi e tedesche

Tuttavia……

- Pro e Contro riguardo alla persistenza dei dati
- Con un tasso di disponibilità del 99.9% +, è probabile che il cloud "non dimentichi nulla"
- Varie copie dei dati (**versioning**) potrebbero essere disponibili in vari siti (potenzialmente distinti e sotto giurisdizioni separate)
- La possibilità di trovare delle copie utili di dati dipende molto dalla qualità del servizio sottoscritto dal target

Per contro……

- La natura "self service" del cloud potrebbe rendere delle preziose informazioni estremamente volatili
- Le risorse allocabili per poche ore in modo "rettangolare" e poi dismesse
  - 20 VM per 1 ora costano come 1 VM per 20 ore
- I dati dell'attività criminosa potrebbero essere sovrascritti in fretta quando le aree disco venissero assegnate ad un altro cliente
- Politiche aggressive di marketing del CSP
  - Es Amazon EC2 spot instances

Per contro……

- Il “modo promiscuo” delle schede di rete potrebbe non funzionare in ambiente cloud poichè l’Hypervisor di norma impedisce lo sniffing del traffico per ragioni di sicurezza
- Una VM controllata dalle forze di polizia posta nello stesso segmento di rete virtuale del target catturerebbe solo il proprio traffico o quello di broadcast
- Su richiesta delle forze di polizia, il CSP potrebbe opporre ragioni tecniche per lasciare questo comportamento inalterato

Per contro……

- I benefici del cloud di abbattere l’investimento iniziale valgono anche per la criminalità
- Gli utenti potrebbero essere più portati a cifrare i dati prima di trasferirli nel cloud
- Formati di dati proprietari del CSP possono comportare trasformazioni mediante strumenti non documentati che potrebbero sollevare rilievi in dibattimento

Un esempio banale

- Amazon S3 implementa un meccanismo di registrazione (log) opzionale dell’accesso agli oggetti
  - Tale registrazione è **disabilitata** per impostazione predefinita
- Le applicazioni che usano Amazon S3 mediante web services possono anche contare su un’opzionale cifratura **AES a 256 bit** (lato server) oppure stoccare oggetti già crittografati (come consigliato per il Cloud pubblico)
  - **DropBox** (www.dropbox.com) usa questa cifratura
  - **BoxCryptor** (http://www.boxcryptor.com/) è un’applicazione per cifrare i dati utente prima di riporli dentro al Virtual Box folder: si hanno così due livelli di cifratura

Considerazioni

- Accedere direttamente ai dati grezzi è di fatto arduo considerata l’impossibilità tecnica di identificare i supporti digitali rilevanti in un datacenter, magari collocato all’estero
- Un’investigazione pertanto dovrà fare affidamento sui dati estratti dal CSP per conto di una parte del processo
  - copie delle VM, file, log di accesso e delle operazioni…
- Necessaria la collaborazione del CSP riguardo alle procedure di acquisizione per soddisfare i principi generali di affidabilità, pertinenza e completezza dei reperti digitali

Considerazioni

- Registrare le informazioni rallenta l'esecuzione dei processi di macchina e costa in termini di spazio disco
  - I log verranno probabilmente tenuti ad un livello minimo, se non concordato diversamente
- L'attività pratica di estrazione dei dati sarà eseguita da amministratori di sistema che potrebbero usare strumenti non di pregio sotto il profilo forense (magari ancora da creare per la tecnologia cloud usata), ma solo script per la manutenzione ordinaria

Considerazioni

- Gli indizi rilevanti potrebbero essere pochi e devono pertanto essere estratti secondo le migliori best practices
- Se possibile, una preventiva interazione di un tecnico forense per condividere procedure e strumenti può evitare di compromettere un'indagine
- Considerata l'estrema variabilità delle procedure in base alle tecnologie adottate dal provider, un accordo dovrebbe essere raggiunto circa la strategia di recupero dei dati ed il loro livello di completezza ed integrità

Considerazioni

- Fare indagini nel cloud richiede elevata consapevolezza dei tecnici forensi nelle seguenti aree
  - Software per la gestione di piattaforme cloud e web services
  - File systems paralleli e database distribuiti
  - Linguaggi di programmazione e tecniche di scripting networking
- Questo per non fare passivo affidamento sui dati forniti dal provider che potrebbe averli estratti senza le procedure e le garanzie necessarie

Considerazioni

- Volatilità nel cloud richiede una collaborazione 24/7/365 ancora più stringente tra le nazioni
  - Variabile tempo in un'indagine di successo diventa ancora più critica
- Delle condivise procedure tecniche applicate all'ambiente cloud contribuirebbero ad assicurare una corretta identificazione ed acquisizione dei reperti, soprattutto in attività congiunte tra paesi diversi

Considerazioni

- Le sfide della forensics in ambiente cloud sembrano essere, qualora considerate, almeno sottostimate
- Di conseguenza i tradizionali strumenti tecnici sin qui utilizzati potrebbero rivelarsi completamente inadeguati in uno scenario di cloud computing

Cloud computing e informatica forense

Il cloud computing può aiutare l'informatica forense?

Cloud computing e informatica forense

- Grazie all'enorme varietà di tecnologie (anche proprietarie), nel Cloud si possono presentare nuove sfide per l'informatico forense
- Le migliori pratiche e le procedure formali consolidate nel tempo che richiedono la completezza nell'acquisizione mediante copie bit-a-bit potrebbero non essere applicabili in ambiente Cloud
  - Riformulazione di **NIST SP 800-86?**
- Tuttavia, la diffusione del cloud computing può offrire alla CF benefici senza precedenti

Problematiche

- I dispositivi elettronici sono sempre più eterogenei, capaci e connessi
- Un caso forense anche di medie dimensioni richiede grandi quantità di spazio disco e potenza di CPU per essere trattato in tempi accettabili

Problematiche dell'IF

- Troppi casi per team di esperti sottodimensionati
  - Carenza di tempo
  - Carenza di risorse
    - Economiche
    - Tecniche
- Necessità di compiere un'analisi globale sul patrimonio informativo dell'indagine e non per reperto
  - Link analysis

- Prospettiva: possibilità di accedere da remoto ai risultati con qualunque dispositivo fisso o mobile

Benefici del cloud computing per l'IF

- L'informatica forense può sfruttare il cloud per
  - Immagazzinare ed analizzare i reperti
  - I tools forensi sviluppati per il cloud potrebbero scalare in maniera orizzontale senza limiti
  - I framenti di ogni reperto (es. i file) potrebbero essere assegnati in parallelo a molte unità di elaborazione e consolidati in un risultato finale
  - I tools potrebbero essere basati su tecnologie open source che minimizzerebbero il problema del lock-in ed aumenterebbero la trasparenza
  - Possibilità di acquistare macchine virtuali per l'informatica forense a tempo

Benefici del cloud computing per l'IF

- Tutto questo in attesa del momento in cui i CSP saranno pronti ad erogare anche un

Forensics as a service

secondo condizioni di fornitura documentate il più possibile e certificate in base alle migliori pratiche forensi

Fine

- Si ringrazia l'Ing. Corrado Federici, collega di dottorato dell'Università di Bologna, per la disponibilità delle slide

- Bibliografia

  - **Federici**,**C** & **Mauro,A.** *Cloud Computing for Government and Military* in Security and Privacy in organizational Cloud Computing, IGI Global 2011 (to be published in 2012)
  - **Reilly & Al**. *Cloud Computing: Forensic Challenges for Law E*Conference, 2010*nforcement* in Internet Technology and Secured Transactions
  - **Taylor,M & Al**. *Forensic Investigation of Cloud Comput*ing *Systems***,** Elsevier 2011
  - **Taylor,M & Al.** Digital evidence in Cloud Computing Systems**,** Elsevier 2010
  - **Barret,D & Kipper,G***: Cloud Computing and the forensic challenges* in Virtualization and Forensics, Syngress 2010
  - **Garfinkel,S.L**. Digital forensic research: the next ten years, DFRWS 2010
  - **Bias, R.** *Elasticity is NOT #Cloud Computing … Just Ask Google.* Cloudscaling.com 2011