E-privacy 2011: Cloud computing e Privacy

Firenze, 3 e 4 Giugno 2011

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

Yvette Agostini
yvette@yvetteagostini.it
http://blog.yvetteagostini.it

Il cloud data storage

stato dell'arte, rischi e tutela della privacy

E-privacy 2011: Cloud computing e Privacy

Firenze, 3 e 4 Giugno 2011

Yvette Agostini

http://blog.yvetteagostini.it

Il cloud data storage

stato dell'arte, rischi e tutela della privacy

- Cloud: qualche definizione
- Tecnologie di interesse
- Quali rischi specifici per i dati?
- Quali contromisure?
- Cenni sugli strumenti crittografici ed il cloud storage

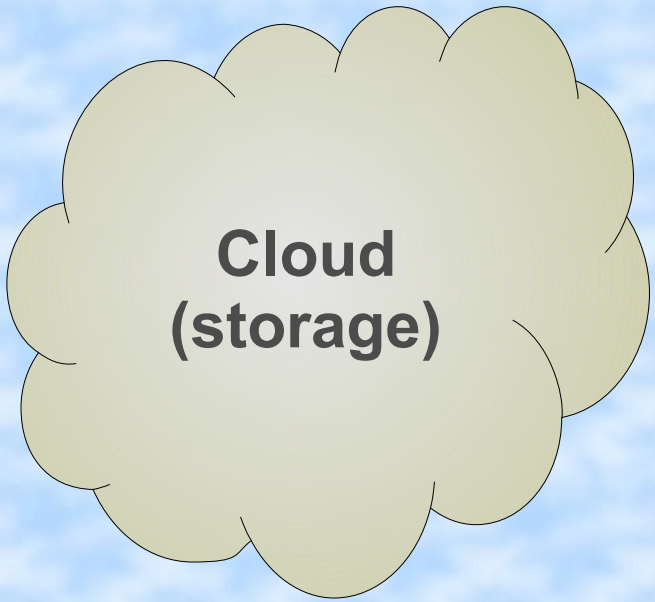
E-privacy 2011: Cloud computing e Privacy

Firenze, 3 e 4 Giugno 2011

Yvette Agostini

http://blog.yvetteagostini.it

Il cloud data storage: stato dell'arte, rischi e tutela della privacy



• **Concettualmente**, la nuvola rappresenta la connettività any-to-any connectivity in una rete

• **Astrazione**: gli effettivi servizi e connessioni interne alla nuvola, necessari per fornire il servizio, non richiedono che pochi interventi manuali per funzionare (dal punto di vista utente)

• La nuvola costituisce una riserva di **risorse e servizi** che possono essere **utilizzati su richiesta**, con incrementi inferiori ai minimi necessari qualora venissero implementati localmente

• Tecnologia abilitante: **virtualizzazione**

[http://cdmi.sniacloud.com/CDMI_Spec/5-Overview_of_Cloud_Storage/5-Overview_of_Cloud_Storage.htm]

Il cloud data storage

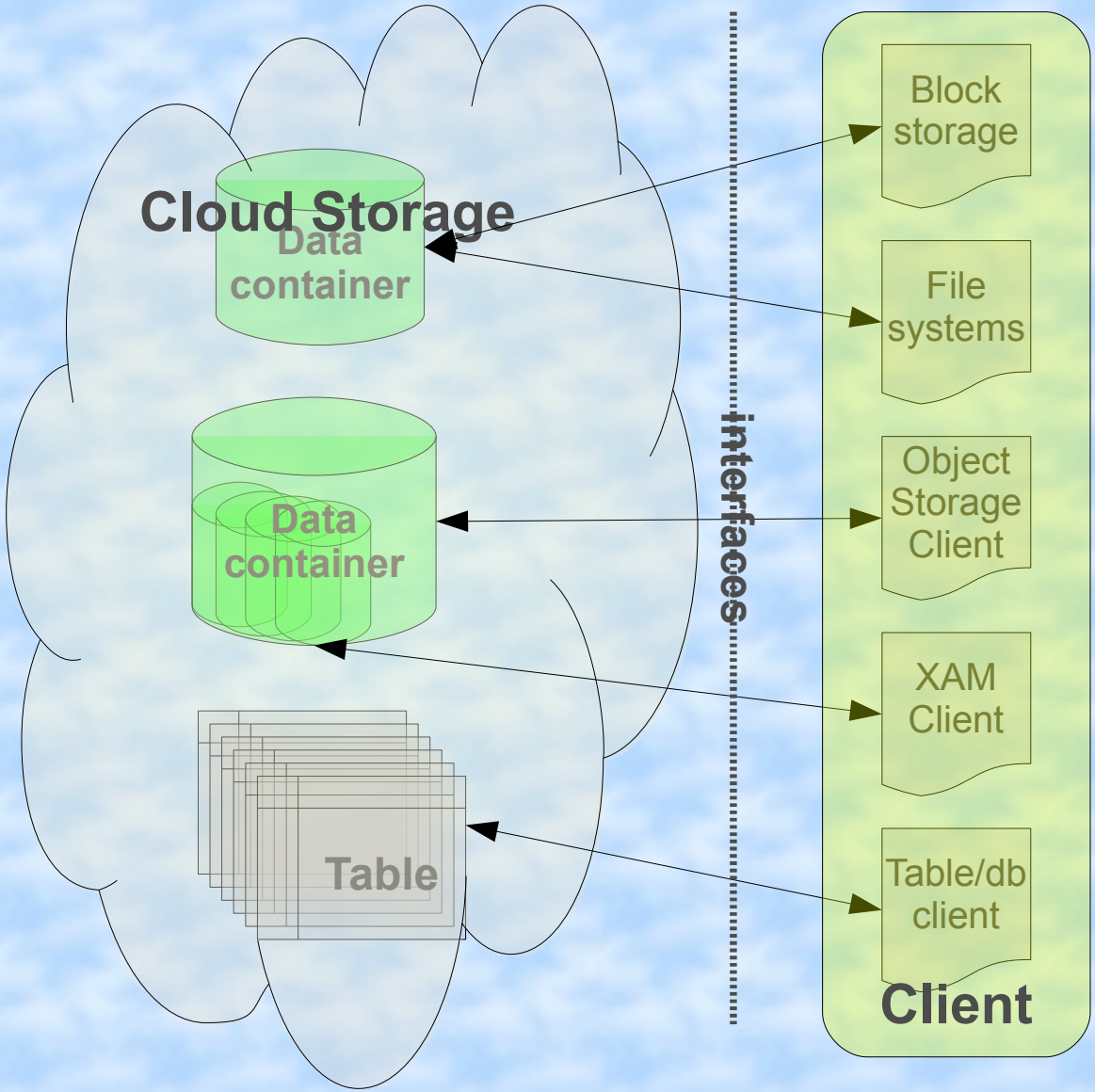
stato dell'arte, rischi e tutela della privacy

Le nuvole (clouds) possono essere:
- private (interne all'organizzazione)
- pubbliche (accessibili ai singoli attraverso internet)
- Ibride (un mix delle caratteristiche delle categorie precedenti)

Data storage as a Service (DaaS)
I fornitori di DaaS mettono a disposizione attraverso la rete lo spazio ed i servizi necessari, opportunamente configurati per fornire un determinato livello di servizio

[http://cdmi.sniacloud.com/CDMI_Spec/5-Overview_of_Cloud_Storage/5-Overview_of_Cloud_Storage.htm]

Il cloud data storage: stato dell'arte, rischi e tutela della privacy



Dove risiedono le criticità?

- client
- Interfacce e transito
- All'interno della nuvola

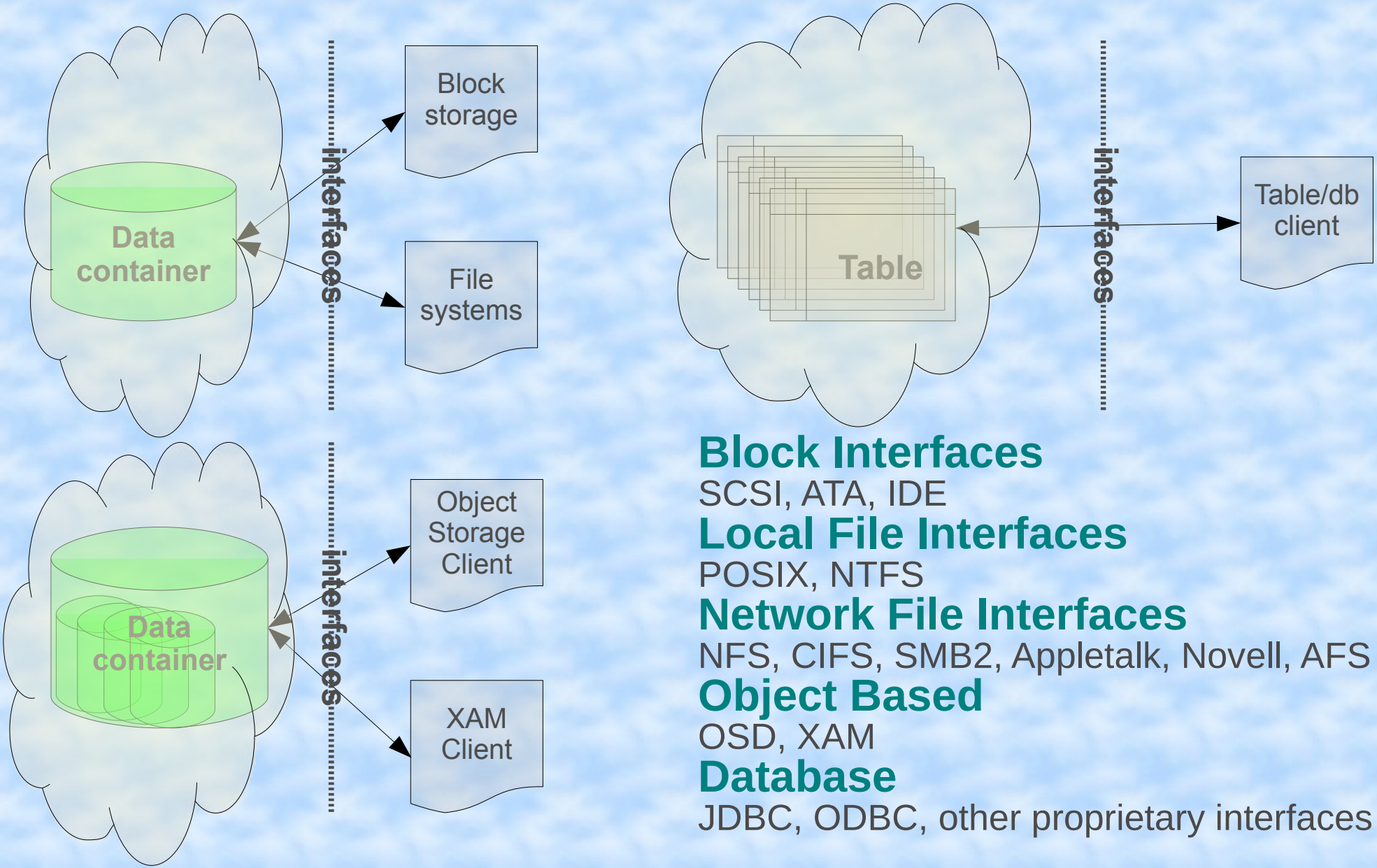
Quali sono le qualità dei dati poste a rischio?

- Confidenzialità
- Integrità
- Disponibilità

Yvette Agostini

http://blog.yvetteagostini.it

Il cloud data storage: stato dell'arte, rischi e tutela della privacy



Block Interfaces
SCSI, ATA, IDE

Local File Interfaces
POSIX, NTFS

Network File Interfaces
NFS, CIFS, SMB2, Appletalk, Novell, AFS

Object Based
OSD, XAM

Database
JDBC, ODBC, other proprietary interfaces

Deduplication Attack

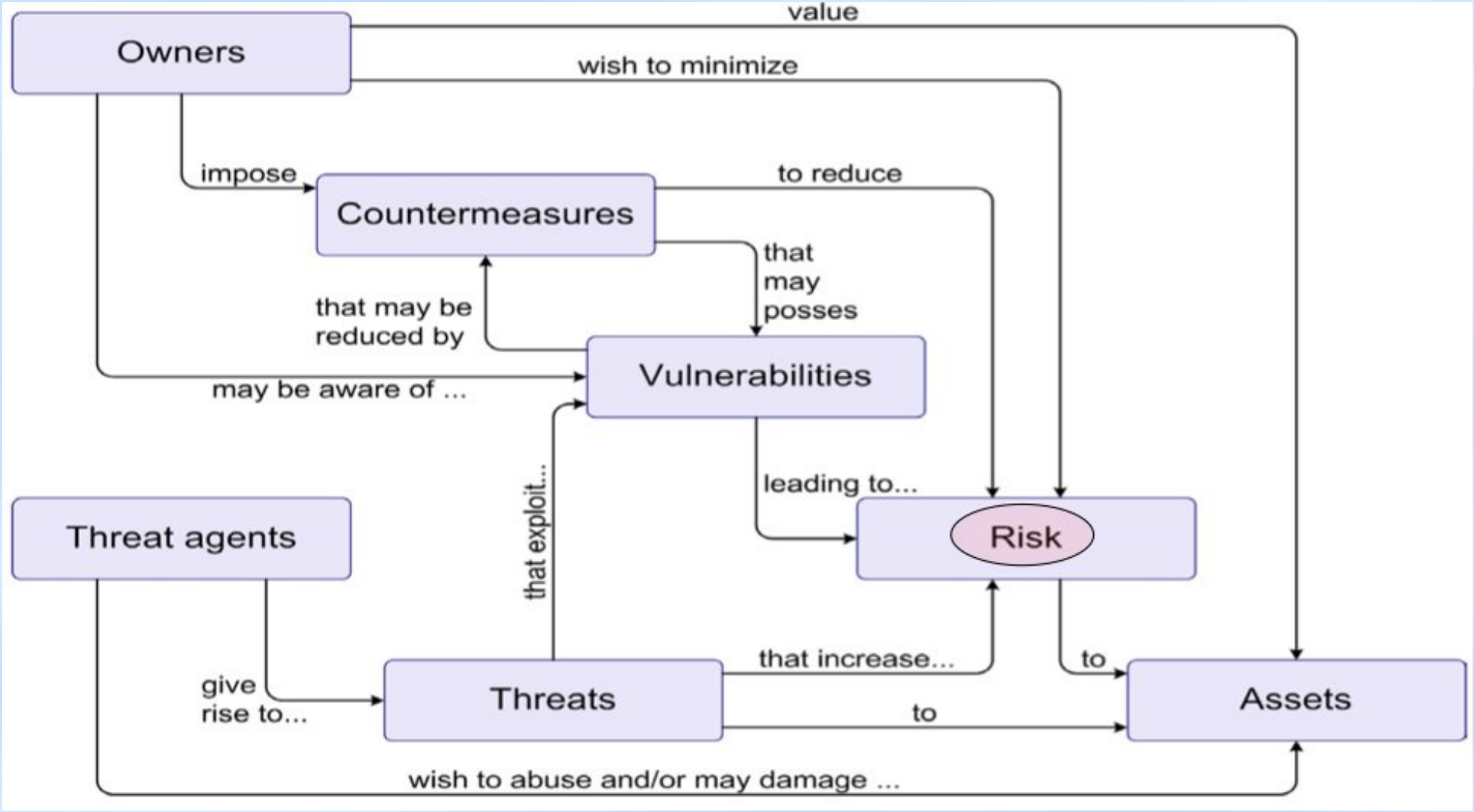
La deduplicazione viene adottata dai fornitori di cloud storage per ridurre lo spazio occupato dai dati, ma espone i dati stessi ad attacchi che consentono di ridurre la riservatezza dei dati

File identification attacks

- Identificazione dei files, mediante attacco alla deduplicazione
- Individuazione contenuti files (una specie di attacco a forza bruta)
- Covert channels (compromesso il client, è facile avere visibilità completa sui file nel cloud storage; non propriamente nel perimetro del cloud...ma d'altronde il cloud implica una ridefinizione del concetto di difesa perimetrale)

[Security of Cloud Storage: Deduplication vs. Privacy Benny Pinkas - Bar Ilan University
Shai Halevi, Danny Harnik, Alexandra Shulman-Peleg - IBM Research Haifa]

Il cloud data storage: stato dell'arte, rischi e tutela della privacy



[ISO/IEC 15408-1:2009, *Information technology -- Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model]*

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

API ed interfacce poco sicure
Le interfacce sw, messe a disposizione dei clienti per gestire e/o interagire con i servizi di storage potrebbero essere poco sicure

Malicious Insiders
Questo tipo di minaccia esiste praticamente in qualsiasi ambiente, ma è amplificata nel cloud qualora vi sia convergenza dei servizi IT e dei clienti in un singolo dominio di gestione, oltre ad una generale carenza di trasparenza nei processi e procedure del fornitore di servizi cloud, così come la scarsa visibilità sugli standard e prassi nellai gestione del personale impiegato dal fornitore Cloud

Problemi legati alla condivisione di tecnologie
I servizi cloud sono scalabili perchè condividono le infrastrutture in architetture multi-tenants, cioè con molti sottoscrittori, di cui non sono note o sono poco chiare le proprietà isolanti

[Cloud Security Alliance, Top Threats to Cloud Computing, Version 1.0, 2010, http://www.cloudsecurityalliance.org/topthreats]

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

Compromissione dei dati
I rischi connessi all'accesso non autorizzato e la modifica/distruzione dei dati sono aumentati nel cloud, per via delle architetture e dell'operatività tipica del cloud

Hijacking dell'account e/o del servizio
Un attaccante potrebbe entrare in possesso di credenziali valide e con esse avere visibilità e possibilità di interazione con attività, transazioni, dati, oltre a poter in alcuni casi redirigere gli utilizzatori verso siti maliziosi e/o utilizzare l'account di accesso al cloud per lanciare altri attacchi (rischio reputazionale)

Profilo di rischio non definito
Le funzionalità dei servizi cloud sono spesso ben pubblicizzate ai clienti, mentre lo stesso non avviene per alcuni dettagli costitutivi l'architettura e gestione del cloud (versioni software, aggiornamenti del codice, prassi di sicurezza, profili di vulnerabilità, tentativi di intrusione, soddisfacimento di standard di sicurezza consolidati, ecc.) ne' per che sarebbero d'aiuto nello stimare il profilo di rischio e nella scelta delle contromisure da adottare per la mitigazione

[Cloud Security Alliance, Top Threats to Cloud Computing, Version 1.0, 2010, http://www.cloudsecurityalliance.org/topthreats]

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

Alcune contromisure suggerite (YMMV):

- Domini disgiunti per la gestione del servizio cloud e per la sua fruizione
- Cifratura dei dati che vengono trasferiti nel cloud storage; non sempre praticabile, non è la panacea, comunque aggiunge carico computazionale
- Canali di trasmissione dati cifrati tra il client ed il cloud, sia per la gestione che per i dati destinati allo storage: ad esempio, implementazione TLS, per avere cifratura del canale di trasporto e autenticazione
- Comunque fondamentale l'accurata classificazione delle informazioni e quindi individuazione dei profili di rischio dei diversi dati.

Cenni sulla crittografia ed il cloud storage

- L' utilizzo appropriato della cifratura (non solo in ambito cloud) dipende da molti fattori
- non sempre è applicabile
- Non è la panacea

Schematizzando:

- **Blind cloud storage**

- **Transparent cloud storage**

Yvette Agostini
http://blog.yvetteagostini.it

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

Blind cloud storage

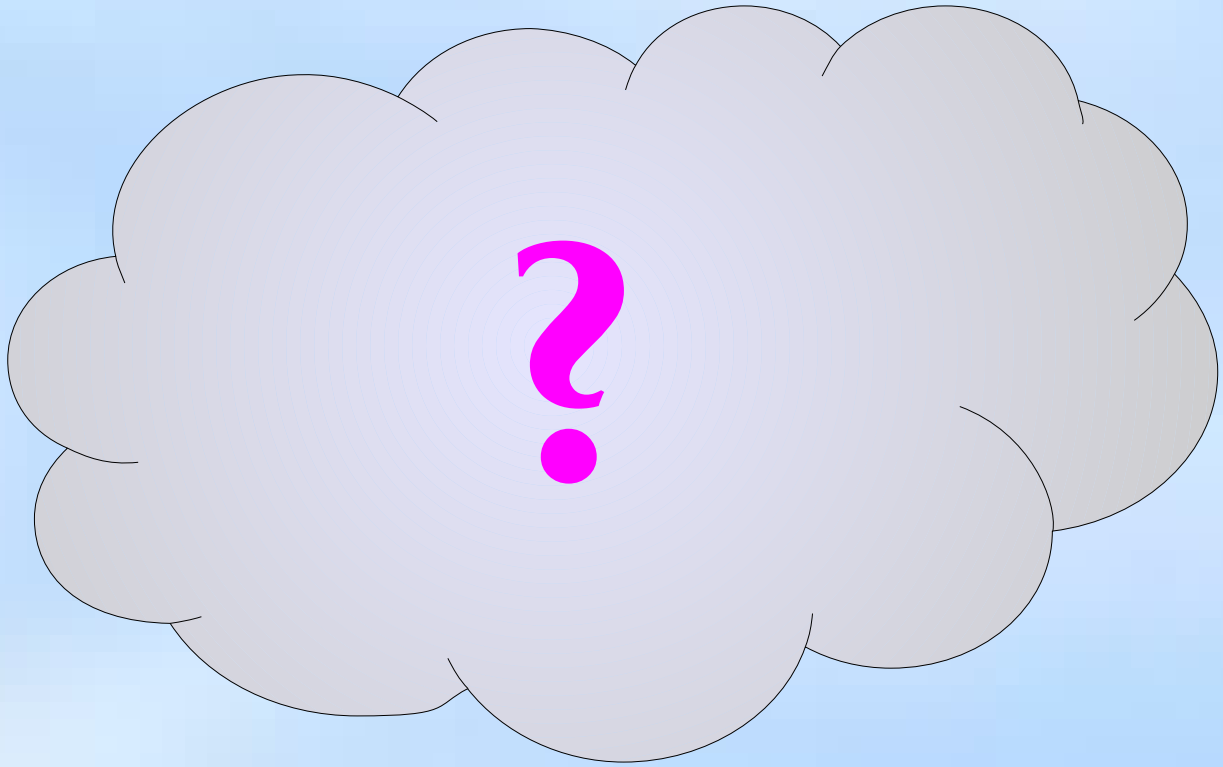
• dati cifrati lato utente, con chiavi crittografiche in suo esclusivo possesso
• il fornitore di cloud storage non ha visibilità su ne' possibilità di accesso ai dati
• non sono possibili, o sono limitati, servizi cloud particolari quali la ricerca full-content nei files, gestione della data retention, conversione di formato, ecc..

Transparent cloud storage

• i dati sono cifrati lato fornitore di servizi cloud e/o esso ha una copia delle chiavi crittografiche
• il fornitore di cloud storage può avere visibilità e possibilità di accesso ai dati
• sono possibili servizi cloud particolari quali la ricerca full-content nei files, gestione della data retention, conversione di formato, ecc..

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

Gli argomenti trattati meriterebbero senza dubbio maggior approfondimento, non possibile in questa sede.
Invito gli interessati a scrivermi per eventuali approfondimenti ed a consultare periodicamente il mio blog, dove rendo disponibili le presentazioni pubbliche, le riflessioni scaturite da specifiche attività, traduzioni e sunti di documentazione inerente il cloud computing



Yvette Agostini
http://blog.yvetteagostini.it

Il cloud data storage: stato dell'arte, rischi e tutela della privacy

Documentazione consultata e consigliata

http://cdmi.sniacloud.com/CDMI_Spec/5-Overview_of_Cloud_Storage/5-Overview_of_Cloud_Storage.htm

SNIA Cloud Storage: Standards and Beyond
http://www.omg.org/news/meetings/tc/dc/special-events/Cloud_Computing/Storage_Network_Industry_Association.pdf

Cloud Security Alliance, Top Threats to Cloud Computing, Version 1.0, 2010,
http://www.cloudsecurityalliance.org/topthreats

Storage Security Best Current Practices (BCPs) Version 2.1.0 Technical Proposal

ENISA Cloud Computing Information Assurance Framework

Angel in our midst: Associative Metadata in Cloud Storage Tom Coughlin and Mike Alvarado

Security of Cloud Storage: Deduplication vs. Privacy Benny Pinkas - Bar Ilan University
Shai Halevi, Danny Harnik, Alexandra Shulman-Peleg - IBM Research Haifa

http://kenai.com/projects/s3-crypto/

Il cloud data storage:
stato dell'arte, rischi e **tutela della privacy**

avv. Valerio Vertua
studio@vertua.it

---

e-privacy 2011
Firenze 3 - 4 giugno 2011

La presente documentazione è messa a disposizione secondo i termini della Licenza Creative Commons: Attribuzione & Condividi allo stesso modo

The following documentation is licensed under the Creative Commons terms: By-sa & Attribution-ShareAlike

Attualità

- *Newsletter n. 345 del 04.02.2011: "... cloud computing sotto la lente del Garante"*
- *Cloud computing e trasparenza on line:! il Garante per la privacy al Forum P.A. 2011*
- *Commissione Europea: consultazione pubblica per permettere a cittadini ed imprese di dire la propria sulle possibili strategie comunitarie in materia di cloud computing*
- *fonti normative: direttiva 95/46/CE e d.lgs. 196/2003 e modifiche... d.l. 13.05.2011 n. 70*

Normativa - aspetti generali

- **sede legale e ubicazione dei server**
  - applicabilità del codice della privacy
  - trasferimento dati all’estero (UE - ExtraUe)
  - accesso ai dati
  - conservazione e cancellazione dei dati

Normativa: applicabilità cod. privacy

- **sede legale e ubicazione dei server**

  (cfr. art. 5 d.lgs. 196/2003)

  - soggetto stabilito nel territorio italiano
  - soggetto stabilito in paese extraUe ma che impiega strumenti situati in Italia (salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'UE)
  - soggetto con sede e server fuori Italia

Normativa: trasferimento dati all’estero

- **paesi UE** (cfr. artt. 37 e 42 d.lgs. 196/2003)
  - notifica al Garante
  - libera circolazione dei dati

a) *dati genetici, biometrici o dati GPS di persone od oggetti;*

b) *dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;*

c) *dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;*

d) *dati trattati con l'ausilio di strumenti elettronici per la profilazione degli utenti;*

e) *dati sensibili in banche di dati per selezione del personale per conto terzi e dati sensibili per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;*

f) *dati in banche dati gestite per il rischio sulla solvibilità economica, la situazione patrimoniale, il corretto adempimento di obbligazioni, comportamenti illeciti o fraudolenti.*

Normativa: trasferimento dati all'estero

- **paesi UE** (cfr. artt. 37 e 42 d.lgs. 196/2003)
  - notifica al Garante
  - libera circolazione dei dati

- **paesi extraUe** (cfr. art. 37 e 43 d.lgs. 196/2003)
  - notifica al Garante
  - dati di pers. giuridiche, enti, associazioni
  - dati di pers. fisiche (principio di necessità)
  - consenso espresso dell'interessato (scritto per dati sensibili)

Normativa: trasferimento dati all'estero

- **paesi extraUe** (cfr. artt. 44 - 45 d.lgs. 196/2003)
  - trasferimento verso paesi che assicurano un livello di protezione adeguato

Normativa: trasferimento dati all'estero

- **paesi extraUe** (cfr. artt. 44 - 45 d.l
  - trasferimento verso paesi che ass
    protezione adeguato

- *Andorra*
- *Argentina*
- *Australia*
- *Canada*
- *Isole Far Oer*
- *Isola di Guernsey*
- *Isola di Man*
- *Isola di Jersey*
- *Stato Israele*
- *Svizzera*

Normativa: trasferimento dati all’estero

- ***Usa - Safe Harbor***
  - Decisione Commissione europea del 26 luglio 2000 n. 2000/520/CE
  - Deliberazione del Garante n. 36 del 10 ottobre 2001 denominata "Autorizzazione al trasferimento verso gli Stati Unti d'America"
  - **principi e "Domande più frequenti" (FAQ) redatti dal Dipartimento del Commercio degli USA in accordo con l'UE al fine di garantire un livello adeguato di protezione dei dati personali trasferiti da persona fisica o giuridica o enti residenti in quest'ultima a soggetti aventi sede negli Stati Uniti**
  - Camera di Commercio Americana - siti web:
    - http://www.export.gov/safeharbor/eu/index.asp
    - http://safeharbor.export.gov/list.aspx

Normativa: trasferimento dati all'estero

- **paesi extraUe** (cfr. artt. 44 - 45 d.lgs. 196/2003)
  - trasferimento verso paesi che assicurano un livello di protezione adeguato
  - adozione clausole contrattuali tipo approvate dalla Commissione UE

Normativa: trasferimento dati all'estero

- **paesi extraUe** (cfr. artt. 44 - 45 d.lgs. 196/2003)
  - trasferimento verso paesi che assicurano un livello di protezione adeguato
  - adozione clausole contrattuali tipo approvate dalla Commissione UE
    - *es.: Decisione della Commissione Europea del 5 febbraio 2010 n. 2010/87/UE (pubblicata su G.U.C.E. L 39/5 del 12.02.2010 e recepita dal Garante italiano con l'Autorizzazione generale n. 35 del 27.05.2010 in G.U. n. 141 del 19.06.2010)*

Normativa: trasferimento dati all'estero

- **paesi extraUe** (cfr. artt. 44 - 45 d.lgs. 196/2003)
  - trasferimento verso paesi che assicurano un livello di protezione adeguato
  - adozione clausole contrattuali tipo approvate dalla Commissione UE
  - regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo

Normativa: trasferimento dati all'estero

- **paesi extraUe** (cfr. artt. 44 - 45 d.lgs. 196/2003)
  - trasferimento verso paesi che assicurano un livello di protezione adeguato
  - adozione clausole contrattuali tipo approvate dalla Commissione UE
  - regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo
  - vietato in tutti gli altri casi

Normativa: accesso ai dati

- **accesso ai dati**
  - utente - affidabilità fornitore servizio cloud data storage
  - autorità pubbliche (es. Patriot Act)
  - dipendenti del fornitore servizio cloud data storage
  - criminali

Normativa: conservazione e cancellazione

- **conservazione dei dati**
  - affidabilità fornitore servizio cloud data storage
  - misure di sicurezza (minime - DPS, idonee)

- **cancellazione dei dati**
  - imposta dalla legge
  - voluta dal titolare
  - affidabilità fornitore servizio cloud data storage

Illeciti e Responsabilità

- *Illeciti Penali* *(trattamento illecito dati; misure di sicurezza)*
- *Illeciti Amministrativi* *(omessa o inidonea informativa dell'interessato)*
- *Responsabilità civile* *(danni cagionati dal trattamento - misure idonee)*

Illeciti e Responsabilità

- *Illeciti Penali* *(trattamento illecito dati; misure di sicurezza)*
- *Illeciti Amministrativi* *(omessa o inidonea informativa dell'interessato)*
- *Responsabilità civile* *(danni cagionati dal trattamento - misure idonee)*

- *Responsabilità Amministrative Enti* *(d.lgs. 231/2001)*

Conclusioni: consigli pratici

- *Analisi strategica delle proprie necessità*
  - *sincronizzazione dei dati*
  - *backup dei dati*

Conclusioni: consigli pratici

- *Analisi strategica delle proprie necessità*
- *Tipologia dei dati da salvare su Cloud*
  - *dati di persone fisiche*
  - *dati di persone giuridiche, enti o associazioni*

Conclusioni: consigli pratici

- *Analisi strategica delle proprie necessità*
- *Tipologia dei dati da salvare su Cloud*
- *Analisi pagine web “Privacy” e “Sicurezza” del fornitore servizio Cloud*
  - *Italia / UE*
  - *Extra UE - (Safe Harbour)*

Conclusioni: consigli pratici

- *Analisi strategica delle proprie necessità*
- *Tipologia dei dati da salvare su Cloud*
- *Analisi pagine web “Privacy” e “Sicurezza” del fornitore servizio Cloud*
- *Informativa dettagliata e completa all’interessato - consenso dell’interessato*

Domande ....

avv. Valerio Vertua

studio@vertua.it