rischi del cloud computing

maurizio pizzonia

dipartimento di informatica e automazione

università degli studi roma tre

ROMA TRE
UNIVERSITÀ DEGLI STUDI

due tipologie di rischi

rischi legati alla sicurezza informatica

- vulnerabilità
- affidabilità
- …

rischi di business

- costi e ricavi
- flessibilità e rigidezze
- …

approccio classico alla sicurezza informatica

risk analysis

fiducia

pianificazione e contromisure

auditing

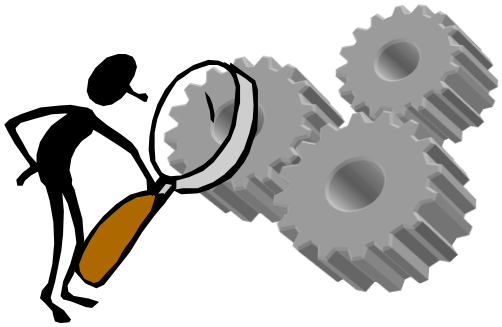
normative e standard

private cloud: aspetti tecnologici

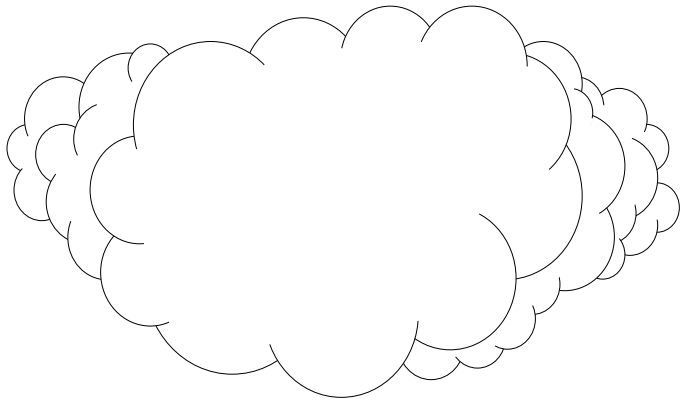
- virtualizzazione delle macchine
- virtualizzazione della rete
- virtualizzazione dello storage
- responsabilità del coordinamento in-house
  - data center, elettricità, sicurezza fisica, coordinamento dei vari attori
- management
  - singoli aspetti tecnologici gestito da vari attori diversi tipicamente in outsourcing

private cloud: sicurezza

- cambiano i profili di rishio
  - maggior importanza della rete
  - maggiore affidabilità e flessibilità
  - rischi di lock-in su specifiche tecnologie di cloud
- sitema pienamente sotto controllo
- l'approccio standard alla sicurezza è applicabile

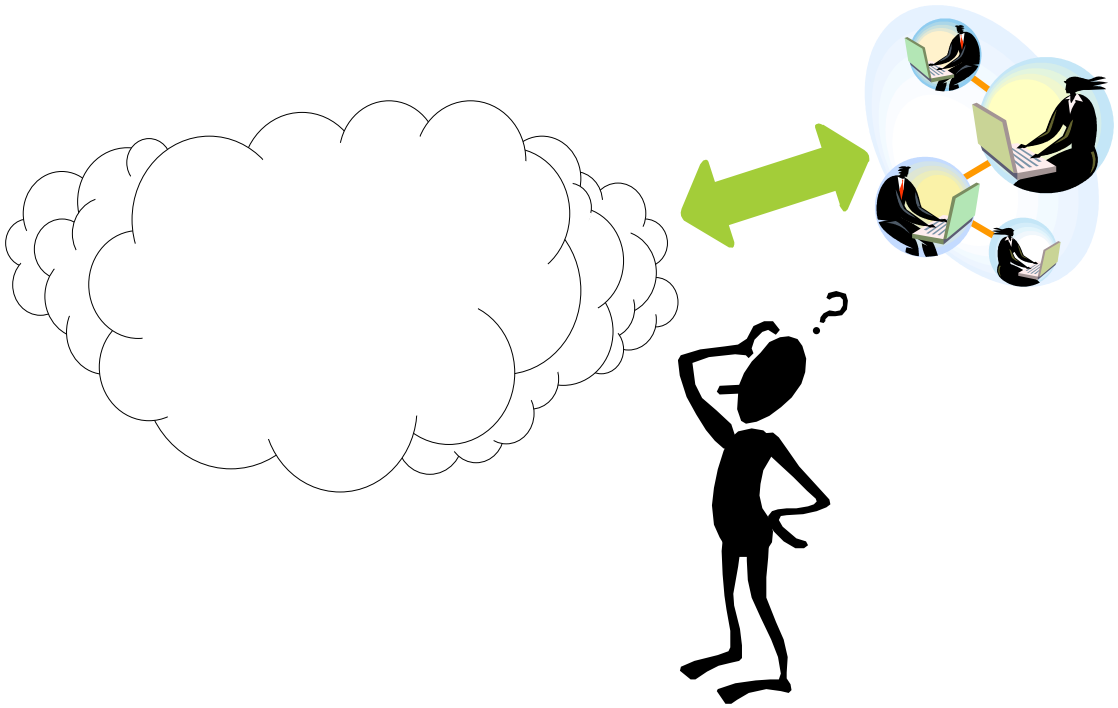


public cloud: aspetti tecnologici



- IaaS
  - macchine virtuali remote
  - interfaccia: shell di root
- PaaS
  - LAMP remoto
    - altra tecnologia (es, Microsoft IIS)
  - interfaccia: files, pannello di controllo, API, una shell limitata
- SaaS
  - applicazione
  - interfaccia: GUI o web

public cloud: sicurezza



- sapere cosa c'è nella nuvola è difficile
- d'altronde la semplicità è un pregio di per sé

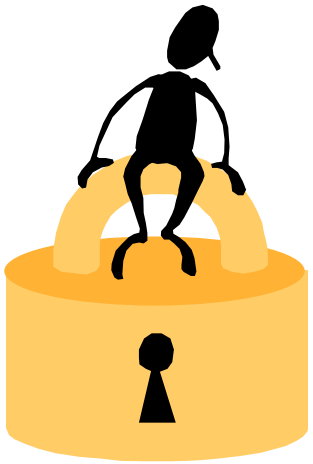
public cloud: problemi

- IaaS
  - come è gestita la sicurezza dell'infrastruttura fisica? da chi?
- PaaS
  - chi amministra la piattaforma?
  - come è gestita la sicurezza dell'infrastruttura fisica? da chi? (vedi reselling)
- SaaS
  - chi ha scritto l'applicazione? con che criteri?
  - come è amministrata la piattaforma? da chi?
  - come è gestita la sicurezza dell'infrastruttura? da chi? (vedi reselling)
- l'unica «interfaccia» per gestire la sicurezza è contrattuale (Service Level Agreement)
  - cioè tutto cio è pane per avvocati!
- approccio black-box?

problemi tradizionali: confidenzialità

- garantita per SLA
  - auditing complesso
- attenzione alla normativa sulla privacy
  - dove sono i dati?

- contromisura: cifratura
  - è un approccio black-box
  - query difficili
  - risolvibile con tecniche “non standard”
    - homomorphic encryption

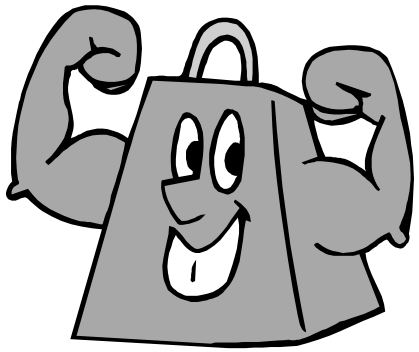


homomorphic encryption

- plain text
  - tabella con due attributi: x, y
  - query: x<y ?
- nel dominio cifrato il predicato di query ha lo stesso risultato
  - tabella cifrata con due attributi: {x}, {y}
  - query: **{x}<{y}** ?
- attualmente meno sicure della crittografia standard
  - da un punto di vista crittoanalitico

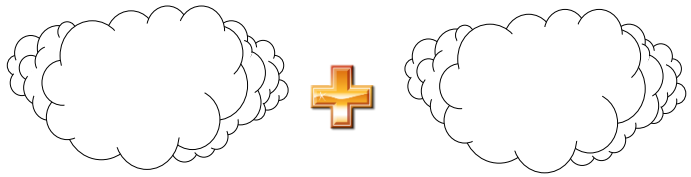
problemi tradizionali: resilienza

- durabilità
  - dicono alta
  - auditing complesso
- disponibilità
  - verificabile con approccio black-box
  - per gli attacchi DDoS probabilmente si
  - per i guasti hw probabilmente si
  - **alta dipendenza dalla affidabilità della rete**
    - uso di VPN acquistate da un ISP con SLA
    - auditing complesso



problemi tradizionali: integrità

- garantita per SLA
  - auditing complesso
- contromisura: replica su due diverse cloud
  - vantaggio anche in termini di disponibilità
  - costoso
  - mancanza di API standard
    - doppio lavoro!



- per grandi moli di dati la completezza è un problema
  - firmare tutto un DB ad ogni inserimento è costoso
  - risolvibile con tecniche “non standard”
    - strutture dati autenticate

inoltre…

- analisi forense spesso impossibile
- omogeneità

  - una vulnerabilità sui sistemi di una cloud ha enorme impatto su tutti gli utenti
- lock-in dell'investimento

  - API non standard

raccomandazioni di ricerca della comunità europea

- BUILDING TRUST IN THE CLOUD
  - Effects of different forms of **breach reporting** on security
  - **End-to-end data confidentiality** in the cloud and beyond
  - **Higher assurance clouds, virtual private clouds** etc
- DATA PROTECTION IN LARGE SCALE CROSS - ORGANIZATIONAL SYSTEMS
  - **Forensics** and evidence gathering mechanisms.
  - **Incident handling** - monitoring and traceability
  - International differences in relevant regulations including data protection and privacy
- LARGE SCALE COMPUTER SYSTEMS ENGINEERING
  - Resource isolation mechanisms - data, processing, memory, logs etc
  - **Interoperability between cloud providers**
  - **Resilience** of cloud computing. How can cloud improve resilience?

- INFRASTRUTTURE CRITICHE