16 - Cloud, IoT, Wireless Networks

I cloud sono utilità per il computing
Il cloud computing è una pool virtuale remota di risorse condivise on-demand che offrono compute, storage, database e servizi di rete che possono essere rilasciati rapidamente a scala

Caratteristiche cloud computing

- Broad network access: capabilities disponibili attraverso la rete tramite meccanismi standard
- on-demand self-service: clienti cloud possono alterare le provvigioni senza interazioni con operatori
- rapid elasticity: abilità di espandere dinamicamente e ridurre le risorse in accordo con la domanda
- shared infrastructure and resource pooling: le risorse dei cloud providers sono pooled per servire molteplici cloud customers.
- measured service: trasparente, fine-grained - pay per usage

Cloud deployment models

Basati sulle identità del provider e ruolo degli users:

- private cloud
- public cloud
- hybrid cloud

Private cloud

- I provider e utente sono parte della stessa organizzazione
- Servizi costruiti per essere compatibili con interfacce cloud generiche (private o pubbliche)
- nessun rischio di vendor lock-in
- Security e data protection nelle mani degli utenti
- costo dell'hardware, spazio e amministrazione simile ad architetture on-premise non-cloud
- private cloud è utile a quelle organizzazioni che hanno sicurezza stretta o regulatory compliances per bisogni di data e computation o laddove i costi di migrazione sono eccessivi

Public Cloud

- provider e user appartengono a organizzazioni diverse
- provider seguono interessi commerciali
- gli utenti non investono nella procurazione, operazione e mantenimento dell'hardware
- possibile rischio di vendor lock-in
- security e data protection dipende dal cloud provider

Hybrid cloud

Servizi da public e private clouds vengono usati insieme nella stessa organizzazione
esempi:

- aumento capacità private cloud con ogni tanto public cloud nei momenti di picco di domande
- delegare certe funzioni come backup dei dati ai public clouds
- leverage della sicurezza dei cloud privati assieme allo scale dei public cloud

Security issues for cloud computing

Molte dei problemi di sicurezza sono simili a quelli dei data center centralizzati
in cloud computing, la responsabilità per la sicurezza è divisa tra utenti, vendors e providers di terze parti.
Virtualizzazione: tecnologia per le cloud infrastructure, se configurata non correttamente potrebbe dare accesso all'utente a informazioni sensibili del cloud.

minacce alla sicurezza

- abuso e utilizzo malizioso del cloud computing
- interfacce o API non sicure
- insider malizioso

- problemi tecnologici condivisi
- data loss o leakage
- account o service hijacking

Cloud security

Ci sono viste differenti sulla sicurezza in un cloud computing setting.
Chi crede che affidare la sicurezza ai cloud provider la renda migliore e chi no.
I problemi sono di due nature:

- problemi dei cloud provider
- problemi dei loro customer
  La responsabilità è quindi condivisa: il provider deve garantire che la loro infrastruttura sia sicura e che i dati e le applicazioni dei client siano protetti. Mentre gli utenti devono adottare misure per fortificare le applicazioni e usare password forti e altri meccanismi di autenticazione.

Cloud provider - Security concern

Il cloud provider è responsabile di:

- Physical security: infrastruttura hardware protetta dagli accessi non autorizzati, furti ecc.
- personnel security: screening di potenziali dipendenti, security awareness e training programs
- identity management: integrazione del sistema di gestione dell'identità del cliente con l'infrastruttura del provider
- infrastruttura sempre aggiornata
- integrità e disponibilità dei dati dell'utente: i dati non devono essere corrotti e devono essere sempre disponibili
- availability dei servizi: le applicazioni cloud degli utenti devono essere disponibili anche quando ci sono power outage, incendi e cyberattacks.
  La natura delle pool di infrastrutture condivise che sono necessarie per facilitare l'elasticità possono essere fonte di altri security concerns (data leakage)
  Le tecnologie di virtualizzazione software che sono necessarie per provvedere isolamento tra gli utenti introduce livelli extra che vanno configurati propriamente e gestiti oltre che resi sicuri.

Data lifecycle

Il controllo della vita dei dati in un ambiente cloud è difficile
Tipicamente è impossibile per un utente:

- controllare dove i dati sono salvati
- controllare se e dove sono i backup
- determinare se i dati che dovrebbero essere stati cancellati lo sono stati effettivamente.
  I cloud providers normalmente sii basano su backup (senza consenso dell'utente) per prevenire data loss accidentali

Cloud user - Security Concern

I cloud users hanno diversi modi per preservare la confidenzialità dei loro dati e minimizzare il rischio di data loss
Tecnologie chiave:

- data encryption
- data replication

Data Encryption

Criptazione di dati sensibili è una difesa critica contro accesso non autorizzato e data theft
i dati criptati devono, se rubati, essere inutili senza le encryption keys
Quali dati hanno bisogno di essere criptati:

- i dati ricadono sotto regulatory compliance requirements, come GDPR, HIPAA ecc..
- i dati sono informazioni identificabili come personali
- i dati contengono informazioni sensibili o proprietà intellettuali
- i dati sono essenziali per il funzionamento dell'organizzazione
  Quando i dati richiedono criptazione:
- quando i dati salvati sono essenziali
- i dati che vengono trasferiti tra il cloud e l'organizzazione o tra cloud (data in-transit)

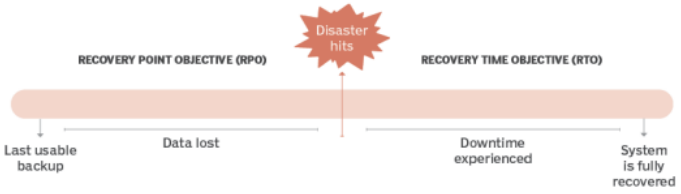
- i protocolli di comunicazione come SSL, TLS, IPSec VPN devono criptare i dati in-transit
  Dove i dati devono essere criptati:
- client-side encryption: encryption dei dati client-side prima dell'upload
- server-side encryption: richiesta al cloud provider di criptare i propri dati prima di salvarli
- cloud application encryption: molti SaaS provvedono criptazione dei dati de facto o opzionale (rischio vendor lock-in)
- cloud security service software encryption: come parte dei loro protection services, le compagnie di sicurezza di terze parti offrono tecnologie di criptazione
  Chi dovrebbe possedere le chiavi di criptazione:
- le encryption key devono essere gestite dal cloud provider o dagli utenti
- possono entrare in fattore le considerazioni sulle regulatory compliance
- indipendentemente d chi possiede le chiavi, il provider deve essere certo che per accedere alle chiavi l'utente deve passare multi-factor authentication e lo storage delle chiavi deve avere backup
- le organizzazioni devono salvare le chiavi in storage media diversi da quello dei dati

Cloud data encryption

I dati sensibili sono sicuri quando sono "at-rest" (devono essere criptati con un forte algoritmo)
Per essere processati i dati criptati devono essere decriptati e questo apre una finestra di opportunità alle vulnerabilità.
Processare i dati criptati senza decriptarli è un vecchio obiettivo della crittografia. Alcuni tentativi: homomorphic encryption, searchable encryption, order-preserving encryption.

Disaster recovery

- Recovery time objective (RTO): è il tempo entro il quale un business process deve essere restored dopo un disastro per evitare gravi conseguenze
- Recovery point objective (RPO): descrive l'intervallo di tempo che passa dall'ultimo backup e un disastro prima che la quantità di dati perduti causi seri danni al business



Data replication strategies

- copia singola: no replicazione
- periodic backups: un backup è una replica ma limitata a disaster recovery e non applicabile ad un accesso normale
- independent copies: qualsiasi copia può essere letta, ma la scrittura è limitata al master che si assume la responsabilità di propagare le modifiche agli slave.
- fully distributed: qualsiasi copia può essere letta, ogni copia che può essere scritta è soggetta a diverse obbligazioni di consistenza

Data consistency models

Come devono comportarsi i dati replicati quando sono comparati alla loro controparte non replicata:

- strict consistency: tutti gli update di un oggetto sono visti da tutte le copie nello stesso ordine 8le copie ritornano sempre il valore dall'ultimo update)
- sequential consistency: gli update ad un oggetto da un qualsiasi writer sono visti da tutte le copie nello stesso ordine
- eventual consistency: se nessun nuovo update è fatto ad un oggetto, eventualmente tutte le copie di quell'oggetto ritorneranno l'ultimo valore aggiornato.

IOT

- edge: estremità di una tipica rete enterprise di IoT-enabled devices, sensori, attuatori, (milioni)
- fog: computing devices vicini all'edge della rete IoT per processare grandi volumi di dati (decine di migliaia)
- core: backbone network che connette reti fog geograficamente lontane
- cloud: provvede lo storage e le processing capabilities per il massive amount di aggregated data originata dall'edge.

IoT security

Elementi dell'IoT security

- tipicamente i gateway implementano secure functions come TLS e IPSec
- unconstrained devices possono o possono non implementare qualche security capability
- constrained devices hanno limitata o nessuna sicurezza
- gateway devices possono provvedere comunicazioni sicure tra il gateway e i device al centro
- unconstrained devices possono comunicare direttamente con il centro e supportano le security functions
- constrained devices che non sono connessi a un gateway non hanno alcuna comunicazione sicura con i central devices.

IoT Embedded systems

- IoT devices che sono sistemi embedded (telecamere di sorveglianza) rappresentano un aumento di rischi sulla sicurezza
- gli embedded devices sono pieni vulnerabilità e non esistono modi semplici
- i produttori di chip hanno forti incentivi a produrre i loro prodotti il più velocemente possibile e meno costosamente possibile
- i device manufacturers scelgono i chip in base al prezzo e features e non ai firmware update.
- l'utente finale potrebbe non avere alcuna possibilità a patchare i sistemi e nel caso ha pochissime informazioni su quando e come farlo.
- il risultato sono centinaia di milioni di device vulnerabili
  Uno sviluppo chiave in IoT security è ITU-Recommendation Y.2067 che definisce specifiche security functions:
- supporto ed identificazione di ogni accesso ai device connessi
- supporto di autenticazioni mutuali o one-way con i dispositivi
- supporto della sicurezza dei dati salvati nei device e gateway
- supporto di meccanismi per proteggere privacy dei device e del gateway
- supporto di self-diagnosis e self-repair oltre a remote maintenance
- supporto di firmware e software update

Security of wireless network

Le wireless networks sono più vulnerabili perchè:

- La comunicazione avviene tramite broadcasting (suscettibile a eavesdropping e jamming)
- sono più suscettibili ad attacchi attivi
- hanno risorse limitate
- sono spesso mobile
- sono più semplici da accedere fisicamente

Wireless network Standards

IEEE 802: un committee che ha sviluppato standard per un grande range di LAN

Wireless LAN security standards

- per privacy 802.11 definiva l'algoritmo Wired Equivalent Privacy (WEP) che è dimostrato contenga diverse debolezze
- La Wi-Fi alliance definisce l'algoritmo Wi-Fi Protected Access (WPA) per sistemare i problemi di WEP
- WEP e WPA sono basati sul RC4 stream cipher
- La versione finale di 802.11i è WPA2 conosciuto come Robust Security Network (RSN)
- RSN si basa su AES block cipher

IEEE 802.11i services

- Autenticazione: provvede mutua autenticazione tra user e authentication server e genera chiavi temporanee per essere usate tra client e l'AP
- Access Control: inforza l'uso delle funzioni di autenticazione, instrada i messaggi propriamente, e facilita lo scambio di chiavi
- Privacy with message integrity: MAC-level data (es. LLC PDU) sono criptati con un messaggio di integrità che assicura che i dati non sono stati alterati.

Minacce alle reti wireless

- Accidental association: WLANs vicine
- Malicious association: falsi access point
- Ad hoc networks: p2p network tra device
- nontraditional networks: Bluetooth o simili
- identity theft: mac spoofing
- man in the middle attack: tra utente e access point
- denial of service attack: particolarmente facile sulle reti wireless
- network injection: access point che sono esposti a routing protocol o network management messages
- sniffing: eavesdrop dei pacchetti particolarmente facile

Security wireless network

Signal hiding techniques:

- disabilitare l'SSD broadcasting dall'access point
- dare nomi complessi all'SSD
- ridurre la forza del segnale
- posizionare gli access point negli edifici lontano dalle finestre e mura esterne
  Altre tecniche
- usare encryption
- antivirus
- cambiare password amministratore di default
- abilitare MAC filtering

Limitare l'accesso alla rete

- port based network access control (PNAC): provvede un meccanismo di autenticazione dei dispositivi che cercano di connettersi ad una lan
- 802.1X è uno standard IEEE per PNAC basato sul Extensible Authentication Protocol (EAP)
- 802.1X può prevenire che gli access point e altri device non autorizzati diventino backdoor non sicure

  Open networks

- Open networks abilitano l'accesso senza rilasciare una password
- Accesso conveniente ma a grande rischio, soprattutto con i wifi pubblici
- La password wifi è usata per criptare i dati dal client al access point
-