ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Seconda Facoltà di Ingegneria
Corso di Laurea in Ingegneria Informatica

IL PROBLEMA DELLA SICUREZZA NEL CLOUD COMPUTING

Elaborata nel corso di: Sistemi Operativi

Tesi di Laurea di:
ALESSANDRO BATTELLI

Relatore:
Prof. ALESSANDRO RICCI

ANNO ACCADEMICO 2011–2012
SESSIONE II

PAROLE CHIAVE

Cloud Computing

Security

Risk assessment

Framework

Indice

Introduzione

Il termine cloud ha origine dal mondo delle telecomunicazioni quando i provider iniziarono ad utilizzare servizi basati su reti virtuali private (VPN) per la comunicazione dei dati. Il cloud computing ha a che fare con la computazione, il software, l'accesso ai dati e servizi di memorizzazione in modo tale che l'utente finale non abbia idea della posizione fisica dei dati e la configurazione del sistema in cui risiedono. Il cloud computing è un recente trend nel mondo IT che muove la computazione e i dati lontano dai desktop e dai pc portatili portandoli in larghi data centers. La definizione di cloud computing data dal NIST dice che il cloud computing è un modello che permette accesso di rete on-demand a un pool condiviso di risorse computazionali che può essere rapidamente utilizzato e rilasciato con sforzo di gestione ed interazione con il provider del servizio minimi. Con la proliferazione a larga scala di Internet nel mondo, le applicazioni ora possono essere distribuite come servizi tramite Internet; come risultato, i costi complessivi di questi servizi vengono abbattuti.

L'obbiettivo principale del cloud computing è utilizzare meglio risorse distribuite, combinarle assieme per raggiungere un throughput più elevato e risolvere problemi di computazione su larga scala. Le aziende che si appoggiano ai servizi cloud risparmiano su costi di infrastruttura e mantenimento di risorse computazionali poiché trasferiscono questo aspetto al provider; in questo modo le aziende si possono occupare esclusivamente del business di loro interesse.

Mano a mano che il cloud computing diventa più popolare, vengono esposte preoccupazioni riguardo i problemi di sicurezza introdotti con l'utilizzo di questo nuovo modello. Le caratteristiche di questo nuovo modello di deployment differiscono ampiamente da quelle delle architetture tradizionali, e i

meccanismi di sicurezza tradizionali risultano inefficienti o inutili. Il cloud computing offre molti benefici ma è anche più vulnerabile a minacce. Ci sono molte sfide e rischi nel cloud computing che aumentano la minaccia della compromissione dei dati. Queste preoccupazioni rendono le aziende restie dall'adoperare soluzioni di cloud computing, rallentandone la diffusione.

Negli anni recenti molti sforzi sono andati nella ricerca sulla sicurezza degli ambienti cloud, sulla classificazione delle minacce e sull'analisi di rischio; purtroppo i problemi del cloud sono di vario livello e non esiste una soluzione univoca.

Dopo aver presentato una breve introduzione sul cloud computing in generale, l'obiettivo di questo elaborato è quello di fornire una panoramica sulle vulnerabilità principali del modello cloud in base alle sue caratteristiche, per poi effettuare una analisi di rischio dal punto di vista del cliente riguardo l'utilizzo del cloud. In questo modo valutando i rischi e le opportunità un cliente deve decidere se adottare una soluzione di tipo cloud. Alla fine verrà presentato un framework che mira a risolvere un particolare problema, quello del traffico malevolo sulla rete cloud.

L'elaborato è strutturato nel modo seguente: nel primo capitolo verrà data una panoramica del cloud computing, evidenziandone caratteristiche, architettura, modelli di servizio, modelli di deployment ed eventuali problemi riguardo il cloud. Nel secondo capitolo verrà data una introduzione alla sicurezza in ambito informatico per poi passare nello specifico alla sicurezza nel modello di cloud computing. Verranno considerate le vulnerabilità derivanti dalle tecnologie e dalle caratteristiche che enucleano il cloud, per poi passare ad una analisi dei rischi. I rischi sono di diversa natura, da quelli prettamente tecnologici a quelli derivanti da questioni legali o amministrative, fino a quelli non specifici al cloud ma che lo riguardano comunque. Per ogni rischio verranno elencati i beni afflitti in caso di attacco e verrà espresso un livello di rischio che va dal basso fino al molto alto. Ogni rischio dovrà essere messo in conto con le opportunità che l'aspetto da cui quel rischio nasce offre. Nell'ultimo capitolo verrà illustrato un framework per la protezione della rete interna del cloud, installando un Intrusion Detection System con pattern recognition e anomaly detection.

Capitolo 1

Il Cloud Computing

1.1 Storia

L'origine del termine cloud computing è sconosciuto, ma sembra provenire dalla pratica di utilizzare un disegno a forma di nuvola per rappresentare una rete negli schemi di telefonia e, negli anni dopo, per rappresentare Internet nei diagrammi di reti di computer.

Il concetto alla base del cloud computing risale agli anni '50, quando i mainframe divennero disponibili al mondo accademico e alle aziende. Comprare un mainframe era molto costoso, e per ricavare il miglior ritorno sugli investimenti era opportuno trovare il modo di permettere a più utenti di accedere allo stesso hardware e di condividere il CPU time.
Negli anni '60 John McCarthy disse che "un giorno la computazione potrà essere organizzata come servizio pubblico".

La grande disponibilità di reti ad alta capacità, la presenza di computer a basso costo e l'utilizzo sempre più diffuso di hardware virtualization, architetture service-oriented, autonomic ed utility computing ha permesso una grande crescita nell'utilizzo del cloud computing.
Amazon, nel tentativo di modernizzare i propri data centres, che utilizzavano fino al 10% della loro capacità la maggior parte del tempo soltanto per lasciar spazio ad aumenti temporanei nell'utilizzo, svolse un ruolo chiave nello sviluppo del cloud computing. Amazon rilasciò Amazon Web Services (AWS) come utility computing nel 2006.

Negli anni successivi vennero rilasciati diversi software open source per il deploy di cloud private ed ibride, e altre grandi aziende del settore, quali IBM, Google e Microsoft, svilupparono software per il cloud computing.[14]

1.2 Caratteristiche del Cloud Computing

- Nel cloud computing gli utenti accedono ai dati, alle applicazioni e altri servizi utilizzando un browser indipendentemente dal dispositivo utilizzato e dalla posizione dell'utente. L'infrastruttura del cloud viene acceduta grazie ad Internet. La spesa per una azienda è considerevolmente abbattuta in quanto le infrastrutture sono offerte da terze parti e non devono essere acquistate per computing occasionale.
- Meno abilità nel campo IT sono necessarie per l'implementazione.
- L'affidabilità del servizio è ottenuta utilizzando diversi siti mirror, sistema adatto per la continuità di business e per il disaster recovery.
- La condivisione delle risorse e dei costi tra un grande insieme di utenti permette un utilizzo più efficiente dell'infrastruttura.
- La manutenzione di applicazioni cloud è semplificata in quanto non devono essere installate nel computer di ogni utilizzatore.
- Utilizzo del modello pay-per-use, grazie al quale l'utilizzo delle risorse può essere misurato e utilizzato come metro di fatturazione.
- La performance può essere monitorata ed è quindi possibile regolarla tramite la scalabilità delle risorse. Al cliente cloud la quantità di risorse utilizzabili spesso appare infinita in quanto può farne richiesta in ogni momento in qualunque quantità.
- La multitenancy (singolo software serve più clienti contemporaneamente, chiamati "tenant) permette la condivisione delle risorse e dei costi su più utenti, permettendo la centralizzazione delle infrastrutture e l'utilizzo efficiente delle risorse. Le risorse vengono assegnate dinamicamente ai vari utenti secondo le richieste che ne fanno. Tuttavia i clienti non sanno dove vengono fisicamente memorizzati i loro dati poiché c'è location independence; questo potrebbe essere un problema

nel caso in cui l'informazione sulla posizione dei dati sia necessaria al contesto del servizio erogato dal cliente.

- Servizio self-service on-demand permette agli utenti di ottenere, configurare ed effettuare il deploy di servizi cloud utilizzando cataloghi di servizi cloud, senza necessità di assistenza da parte dell'azienda provider. Questo requisito porta i provider cloud a stilare template per servizi che loro offrono, da inserire in un catalogo di servizi. Ogni template contiene le configurazioni predefinite necessarie per impostare un servizio cloud pronto all'uso.

- Tecnologie di virtualizzazione permettono la condivisione di server e dispositivi di memoria, facilitano inoltre la migrazione di applicazioni fra più server fisici.[17]

1.3 Architettura Cloud

L'architettura di un sistema cloud può essere suddivisa in due macro parti: il front-end ed il back-end. Il front-end è ciò che l'utente vede e con cui interagisce, è eseguito nel computer del cliente e consiste nell'applicazione necessaria ad accedere al cloud, mentre il back-end è il nucleo del sistema, dove tutte le risorse e le unità di computazione che servono per far funzionare il sistema giacciono.

Guardando figura 1.1, il layer di cloud software infrastructure provvede le risorse base che sono offerte come servizi ai layer sovrastanti: risorse computazionali (in genere environment di macchine virtuali), memoria e comunicazione su rete. Questi servizi possono essere utilizzati individualmente, come succede tipicamente con i servizi di memorizzazione, ma sono spesso offerti in "bundle". Questi servizi offerti assieme sono spesso riferiti come Infrastructure as a Service (IaaS).

Il layer di cloud software environment fornisce servizi al livello di piattaforma di applicazione:

- un ambiente di sviluppo ed esecuzione per servizi e applicazioni scritti in uno dei linguaggi supportati;

- dispositivi di memoria;

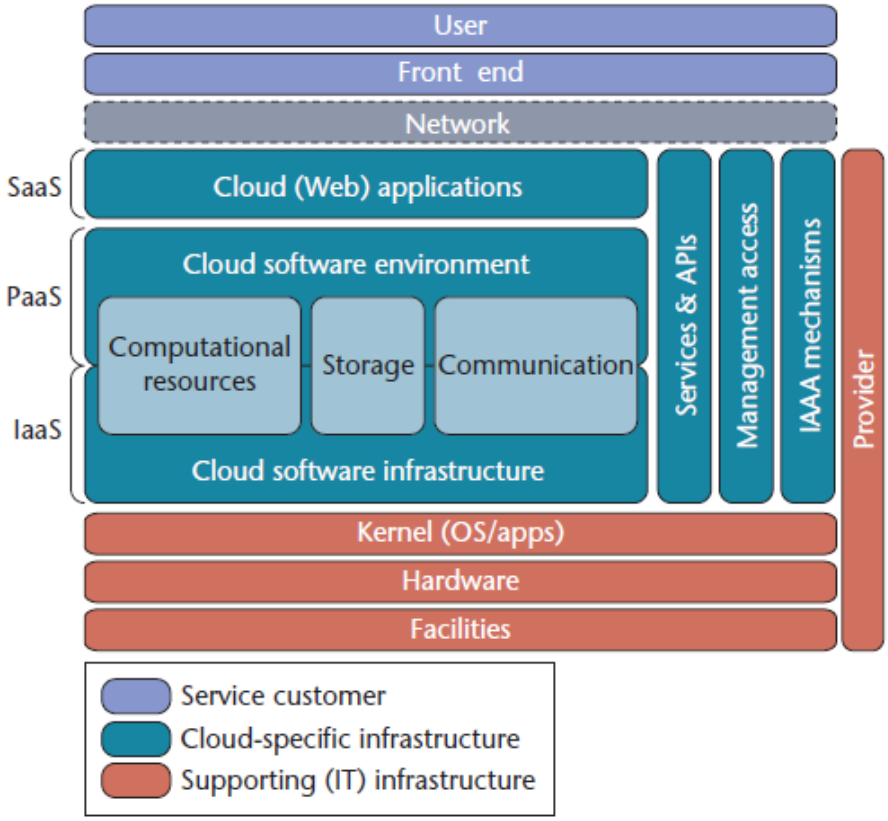


Figura 1.1: Architettura cloud.

- infrastruttura di comunicazione;

Questo layer corrisponde al Platform as a Service (PaaS).

Le applicazioni sovrastanti, segnate come Cloud applications in figura 1.1, rappresentano il Software as a Service (SaaS) e sono le applicazioni (in genere implementate come Web Service) accessibili ai clienti del cloud.

Una delle tecnologie su cui si basa il cloud computing è la virtualizzazione. Una macchina virtuale è il contenitore logico di un sistema operativo ospite e delle applicazioni che esso esegue. E' memorizzata come una immagine di disco e quindi può essere trasferita da un server ad un altro. L'hypervisor

è ciò che gestisce le macchine virtuali eseguite sullo stesso server fisico, e presenta ai sistemi operativi ospite delle viste virtualizzate dell'hardware fisico e delle risorse. Si occupa inoltre del set-up, dello spegnimento e della migrazione delle macchine virtuali di cui è responsabile.

1.4 Modelli di servizio

Il cloud computing offre servizi secondo tre modelli fondamentali: Infrastructure as a service (IaaS), Platform as a service (PaaS), e Software as a service (SaaS), in cui la IaaS rappresenta il livello base e ogni modello superiore astrae dai dettagli del modello inferiore.

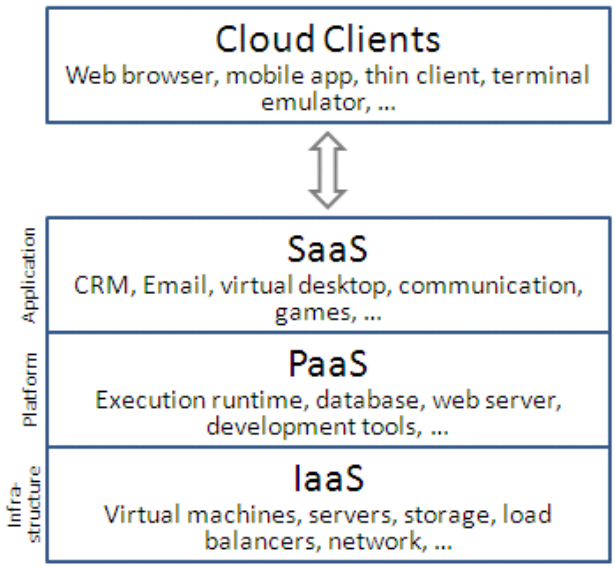


Figura 1.2: Layer cloud

I cloud client consistono in hardware o software che fanno affidamento sul cloud computing per la distribuzione di applicazioni. Sono i clienti del provider cloud.

Una cloud application offre **SaaS** su Internet, eliminando la necessità di installare ed eseguire l'applicazione sul sistema dell'utente finale. Nel modello SaaS il cloud provider installa l'applicazione software nel cloud e gli

utenti utilizzano i cloud client per accedervi. Caratteristiche importanti di questo tipo di offerta è l'accesso e la gestione di software remotamente tramite Internet e la scalabilità delle applicazioni cloud. Le task in un cloud possono essere clonate a tempo di esecuzione su diverse macchine virtuali per soddisfare i requisiti di risorse. Dei load balancers si occupano di distribuire il lavoro su diversi insiemi di macchine virtuali, tutto in modo trasparente all'utente cloud. Le cloud application possono essere multitenant, cioè ogni macchina serve più di un utente cloud, questo per utilizzare efficientemente le risorse messe a disposizione, poiché se venissero utilizzate da un singolo utente per volta rischierebbero di rimanere per la maggior parte inutilizzate.

I servizi Platform **(PaaS)** offrono una piattaforma di computing utilizzando l'infrastruttura cloud. L'ambiente offerto tipicamente ha già tutte le applicazioni necessarie al cliente. In questo modo il cliente non deve occuparsi di comprare, installare e configurare diversi hardware e software per eseguire i suoi programmi. Tramite questo servizio gli sviluppatori possono ottenere tutti gli ambienti di sistema necessari per il ciclo di vita dei loro software.

I servizi di Infrastructure **(IaaS)** offrono l'infrastruttura necessaria come servizio, cioè computer, sia fisici che virtualizzati e altre risorse. Le macchine virtuali sono eseguite dall'hypervisor e diversi hypervisor dentro lo stesso cloud possono ridimensionare i servizi a seconda dei requisiti del cliente. Altre risorse offerte come Infrastructure sono firewall, load balancer, range di indirizzi IP e virtual local area networks.

Il cliente non deve comprare i vari server, centri di dati o risorse di rete di cui può necessitare, ma deve occuparsi di installare, patchare e manutenere le immagini di macchine virtuali e gli applicativi di cui può necessitare.

Un altro vantaggio chiave è che il cliente deve pagare solo per la durata del tempo in cui utilizza il servizio. Come risultato il cliente ottiene un servizio molto velocemente a costo basso.

1.5 Modelli di deployment del servizio Cloud

Quando si offre una soluzione di cloud computing, è indispensabile decidere quale modello deve essere implementato. Ci sono quattro tipi di cloud computing: public cloud, private cloud, community cloud e hybrid cloud.

1.5.1 Public cloud

Il **public cloud** permette agli utenti di accedere al cloud tramite web browser. Gli utenti pagano solo per il tempo di utilizzo del servizio, tuttavia i cloud pubblici sono meno sicuri rispetto agli altri modelli poiché il mezzo utilizzato, Internet, è intrinsecamente insicuro. La maggior parte dei problemi di sicurezza avviene in questo tipo di cloud anche perché il cliente si rivolge a terze parti per la gestione dei propri dati, perdendone il controllo fisico. Standard di sicurezza, accordi, licenze e suddivisione precisa di ruoli e responsabilità deve avvenire tra cliente e provider per preservare i dati.

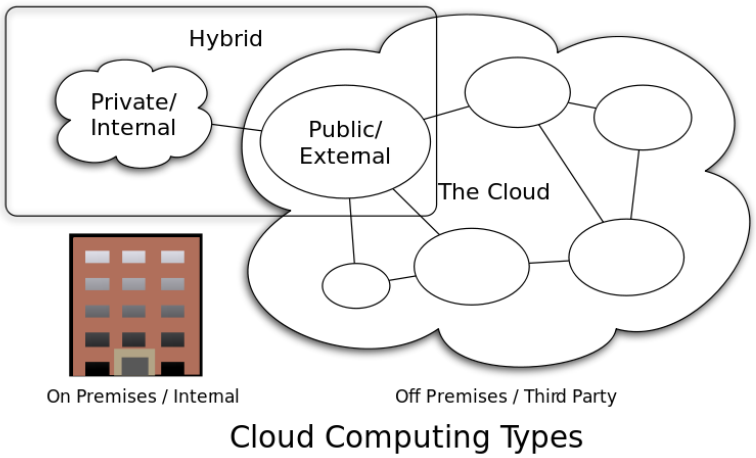


Figura 1.3: Tipi di cloud computing

1.5.2 Private cloud

Una soluzione del tipo **private cloud** prevede il deploy di un cloud all'interno dei confini di una azienda. Il vantaggio principale è la facilità con cui si gestisce la sicurezza, la manutenzione e gli aggiornamenti, e provvede inoltre più controllo sul deployment e sull'utilizo. I cloud privati possono essere comparati alle intranet. Rispetto ai cloud pubblici, dove tutte le risorse e le applicazioni sono gestite dal service provider e sono condivise dagli utenti del cloud, nei cloud privati questi servizi sono messi a disposizione degli utenti a livello aziendale e le risorse sono gestite dall'organizzazione stessa.

La sicurezza è più alta in quanto solo gli utenti dell'organizzazione hanno accesso al cloud privato. A questo tipo di soluzione manca uno dei vantaggi principali del cloud computing per il cliente, cioè l'essere indipendenti dalla costruzione e manutenzione di una nuova infrastruttura di computing. Una azienda che decide di adottare un cloud privato dovrà infatti spendere considerevoli risorse per implementarlo.

1.5.3 Community cloud

Nel **community cloud** le infrastrutture sono condivise tra diverse organizzazioni di una specifica comunità con interessi comuni, può essere gestita internamente o da terze parti, ospitata internamente o esternamente. I costi sono divisi tra meno utenti rispetto ad un cloud pubblico, perciò il costo per ogni utente sarà maggiore e viene perso questo vantaggio caratteristico dei cloud pubblici.

1.5.4 Hybrid cloud

L'ultimo tipo di cloud, lo **hybrid cloud**, è composto da due o più cloud, privati, community o pubblici, che rimangono entità uniche ma sono legate assieme, permettendo di offrire i benefici di un modello di deployment multiplo. Utilizzando il modello hybrid cloud le aziende e le persone sono in grado di ottenere diversi gradi di fault tolerance combinati con l'usabilità immediata delle risorse ospitate in locale, perciò senza la dipendenza della connettività alla rete esterna. Le architetture hybrid cloud necessitano sia di risorse ospitate in locale che di una infrastruttura cloud off-site. In genere una cloud privata si appoggia ad una cloud pubblica; permette all'organizzazione di soddisfare le proprie necessità utilizzando la cloud privata e di utilizzare quella pubblica in caso di picchi di necessità di risorse computazionali.

1.6 Problemi

Il cloud computing offre innumerevoli vantaggi ma ci sono aspetti che ne impediscono la diffusione ad ampia scala.

Privacy

Il modello cloud è stato criticato per la facilità con cui le compagnie provider dei servizi cloud controllano e quindi monitorano a piacere, legalmente o illegalmente, le comunicazioni e i dati memorizzati dei propri utenti. La privacy dei dati non è sicura poiché, visto che il provider utilizza tecnologie come la virtualizzazione, i dati possono non rimanere nello stesso sistema, nello stesso centro di dati o addirittura nello stesso cloud nel caso in cui il provider si appoggi a sua volta ad un servizio cloud. Questo può portare a complicazioni legali riguardo la giurisdizione. Devono essere applicate misure di protezione dei dati, quali criptazione, per mantenere sicura la privacy.

Compliance

Visto che i servizi erogati da un cloud possono essere sfruttati da tutto il mondo esistono problemi di conformità. Ad esempio clienti nell'Unione Europea che firmano un contratto con un cloud provider proveniente dal di fuori dell'Unione Europea devono aderire ai regolamenti dell'UE riguardo l'esportazione di dati personali.

Le agenzie federali americane utilizzano un processo chiamato FedRAMP (Federal Risk and Authorization Management Program) per valutare e autorizzare prodotti e servizi cloud. Il FedRAMP consiste in un sottoinsieme di controlli di sicurezza presenti nel NIST Special Publication 800-53 scelti specificatamente per provvedere protezione in ambienti cloud.

Legalità

Assieme al cloud computing sono sorti anche problemi di tipo legale, quali violazione di trademark, problemi di sicurezza e condivisione di dati personali.

Caso eclatante è la confisca di Megaupload, durante la quale il governo americano ha considerato i dati confiscati non più di proprietà dei clienti, accedendo ai dati personali di un utente che non aveva nulla a che fare con il motivo di confisca di Megaupload.[6]

Un problema importante riguarda la proprietà dei dati. Se una azienda

cloud è la proprietaria dei dati, la azienda ha certi diritti. Se una azienda cloud è invece semplicemente un "custode" dei dati, diversi diritti si applicano. Molti Termini di Utilizzo non parlano di questa importante questione.

Open standards

Molti cloud provider offrono API che sono ben documentate ma che sono uniche alla loro implementazione e quindi non interoperabili. Esistono un numero di standard aperti che mirano a portare interoperabilità e portabilità ma tutt'ora la migrazione da un provider ad un altro è molto difficile se non impossibile.

Sicurezza

I meccanismi di protezione tradizionali non si rivelano efficaci con questo nuovo modello computazionale. La preoccupazione da parte delle aziende riguardo la sicurezza del cloud computing è fra le cose che sta ritardando l'adozione diffusa di soluzioni cloud. Questo aspetto verrà discusso più a fondo durante questo elaborato.

Abuso

I clienti possono comprare servizi cloud per utilizzi ragguardevoli. I provider non possono tenere conto delle attività di tutti i loro utenti per rispetto della privacy, perciò è possibile che una infrastruttura venga noleggiata per essere utilizzata come base da cui lanciare attacchi.

Capitolo 2

La sicurezza nel cloud computing

"Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente."[16]

I termini information security e computer security sono spesso usati intercambiabilmente poiché condividono gli scopi comuni di mantenere alcune proprietà dell'informazione, quali confidentiality, integrity e availability.

La confidentiality consiste nel prevenire la rivelazione delle informazioni a individui o sistemi non autorizzati. La confidentiality è necesasria per mantenere la privacy delle persone che posseggono le informazioni.

La integrity significa che i dati non possono essere modificati senza che questo sia noto.

La availability mira a rendere i dati disponibili in qualunque momento siano necessari.

Per ottenere un sistema sicuro si procede in diverse direzioni. Dal punto di vista organizzativo, si progettano ruoli e si assegnano responsabilità ben precise per ogni utilizzatore del sistema. In questo modo l'area di attacco di un ipotetico malfattore è più ristretta e definita, e allo stesso tempo in corrispondenza di un attacco si ha idea da quale direzione l'attacco arrivi

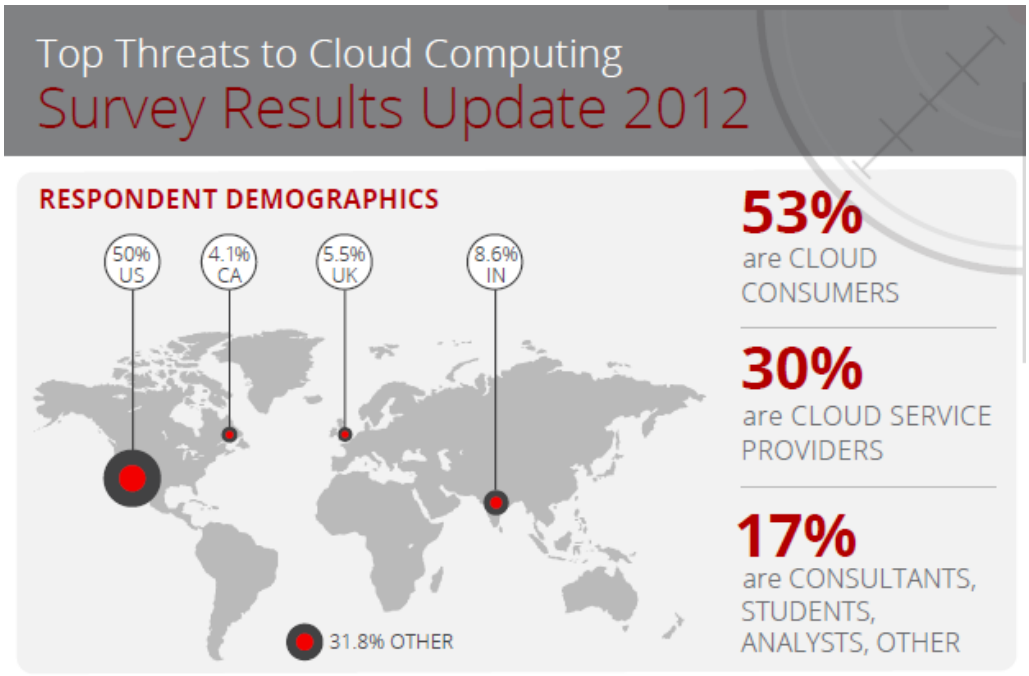
(un attacco può arrivare anche da un membro stesso della società, chiamato insider). Dal punto di vista tecnologico si utilizzano diversi sistemi di protezione adatti al contesto che si vuole proteggere.

Per poter applicare soluzioni di sicurezza ai problemi del sistema, prima è bene definire quali siano i problemi, e per far questo si effettua una analisi di rischio. Il National Institute of Standards and Technology (NIST) definisce rischio come "a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization". Il rischio è quindi definito in funzione della probabilità che una minaccia sfrutti una vulnerabilità e delle conseguenze (impact) di questo evento sulla organizzazione.
Una vulnerabilità invece è definita come "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy".[15]
Nelle sezioni successive verrà effettuata una analisi di rischio e verranno evidenziate alcune vulnerabilità per quanto riguarda il cloud computing. Per ogni rischio verranno evidenziate le vulnerabilità che lo riguardano, la probabilità che una minaccia sfrutti con successo una vulnerabilità, i beni che vengono impattati dallo sfruttamento della vulnerabilità e infine un livello di rischio dipendente dalle caratteristiche precedenti.

2.1 Il problema della sicurezza nel cloud computing

Come visto, il cloud computing ha molti pregi. Offre flessibilità, deploy di servizi veloce e permette alle aziende di risparmiare trasferendo dati, informazioni e infrastrutture ad un provider di terze parti. In questo modo l'azienda non si deve preoccupare più di gestire le infrastrutture ma può concentrarsi sullo svolgere attività di sua competenza.

Cosa succede però ai dati quando sono trasferiti offsite, fuori dal controllo fisico o logico? Visto che i cloud provider non rivelano la posizione dei dati è quasi impossibile dire dove sono immagazzinati, perciò l'azienda perde il controllo sulla sicurezza fisica dei dati. Inoltre in un cloud pubblico tutti



condividono le risorse in uno spazio comune, ad esempio un pool condiviso, fuori dalla portata dell'organizzazione; è al caso limite possibile che i dati di una certa organizzazione siano immagazzinati assieme ai dati di un'organizzazione concorrente. Se le informazioni sono criptate, chi è in controllo delle chiavi di criptazione/decrittazione, il provider del cloud o il cliente? Questo e molti altri problemi necessitano di risposte, e questo è uno dei motivi più importanti per cui il cloud computing non si è ancora diffuso in maniera estesa. Le aziende sono riluttanti ad adoperare una soluzione che si basa sul cloud computing perché non esiste uno standard a cui i provider aderiscono che assicura un certo livello di sicurezza, e lo standard non esiste perché i problemi che affliggono il cloud computing sono molteplici e non di semplice soluzione. A questo riguardo è nato nel 2009 un gruppo chiamato Cloud Security Alliance, che può contare tra i fondatori eBay e ING, che si occupa di effettuare rilevazioni, educare i provider cloud e provvedere certificazioni per quanto riguarda la cloud security.[9]

L'adozione del cloud computing non ci permette di trattare i soliti pro-

blemi di sicurezza allo stesso modo in cui si faceva con altre tecnologie. Per capire quale sia il delta che il cloud computing apporta rispetto ai problemi di sicurezza dobbiamo analizzare come il cloud computing influenza i problemi di sicurezza conosciuti. [4] Come vengono influenzati i fattori di rischio (probabilità, impatto) dal cloud computing? Dal punto di vista di un utente le conseguenze non sono influenzate dall'utilizzo del cloud: il costo ultimo di, ad esempio, una breccia nella riservatezza delle informazioni, è esattamente lo stesso indipendentemente se la breccia è avvenuta in un ambiente cloud o in una infrastruttura IT convenzionale. Per un provider cloud le cose sono differenti in quanto se prima i sistemi di computazione erano separati, ora un evento di perdita potrebbe avere un impatto molto più largo.
Ciò che l'adozione del cloud computing influenza maggiormente è la probabilità di un evento dannoso. Il cloud computing cambia fortemente il fattore

di vulnerabilità, variando il livello di accesso e le modalità di attacco disponibili per un malintenzionato.

Esistono vulnerabilità specifiche al cloud perciò devono esistere fattori insiti alla natura del cloud computing che rendono una vulnerabilità specifica al cloud.

Verrano elencate ora le tecnologie e gli aspetti che interessano il cloud computing dal punto di vista della sicurezza.

Il cloud computing si basa su funzionalità provvedute da diverse tecnologie base:

Servizi e applicazioni web. Il SaaS e il PaaS sono impensabili senza applicazioni web e servizi web, in quanto le offerte SaaS sono tipicamente implementate come applicazioni web mentre le offerte PaaS provvedono ambienti di esecuzione e sviluppo per applicazioni web. Per quanto riguarda le offerte IaaS, le API e i servizi utilizzati per accedervi sono tipicamente implementati come applicazioni/servizi web.
Virtualizzazione. Queste tecnologie si basano pesantemente sulla virtualizzazione e visto che PaaS e SaaS si basano su una struttura IaaS di supporto, l'importanza della virtualizzazione si estende anche a questi modelli di servizio.
Crittografia. Molti requisiti per la sicurezza nel cloud computing possono essere risolti soltanto usanto tecniche crittografiche.

Nella descrizione delle carattersitiche cloud, il NIST delinea gli attributi che permettono al cloud computing di offrire servizi *from the conveyor belt* utilizzando economia di scala:

Self-service on-demand. Gli utenti possono ordinare e gestire servizi senza interazioni umane direttamente dal portale del provider, sfruttando interfacce di gestione. Il commissionamento e il decommissionamento avviene automaticamente da parte del provider.
Accesso semplice. I servizi cloud sono acceduti tramite la rete utlizzando protocolli standard.
Pooling delle risorse. Le risorse di computazione utilizzate per erogare i servizi sono realizzate utilizzando un'infrastruttura omogenea condivisa tra tutti gli utenti.

Elasticità rapida. Le risorse provvedute ad un servizio possono essere ridimensionate rapidamente.
Servizio misurato. L'utilizzo delle risorse è costantemente monitorato e riportato per soddisfare il modello di business pay-as-you-go.

Le tecnologie che enucleano il cloud computing - applicazioni web e servizi, virtualizzazione e criptografia - e le caratteristiche descritte da NIST - Self-service on-demand, accesso semplice, pooling delle risorse, elasticità rapida, servizio misurato - portano con sé vulnerabilità insite alla caratteristica o alla tecnologia, che verranno quindi inevitabilmente trasferite al cloud. Oltre a queste vulnerabilità ne esistono di nuove, nate proprio con il cloud computing (esempio EDoS), di cui si dovrà tenere conto.

2.2 Classificazione delle vulnerabilità

Vulnerabilità dell'hypervisor

Gli attacchi al layer hypervisor sono molto attraenti per un attaccante: l'hypervisor di fatto controlla completamente le risorse fisiche e le macchine virtuali eseguite su di esse, perciò ogni vulnerabilità a questo livello sono estremamente critiche. Sfruttare l'hypervisor significa sfruttare potenzialmente ogni macchina virtuale. Il primo proof of concept di un attacco contro l'hypervisor è stato fatto da King et al nel paper [18], dove gli autori introducono il concetto di rootkit virutal machine-based. Al tempo di pubblicazione alcune vulnerabilità furono identificate negli hypervisor più popolari [1] che potevano essere sfruttate senza diritti amministrativi.

Uno scenario tipico raggiunto sfruttando una vulnerabilità dell'hypervisor è quello del 'guest to host escape', ad esempio 'Cloudburst', una vulnerabilità di VMware documentata in [10]. Un altro scenario è il 'VM hopping': un attaccante hackera una macchina virtuale utilizzando metodi standard e poi - utilzzando vulnerabilità dell'hypervisor - prende il controllo di altre macchine virtuali in esecuzione sullo stesso hypervisor.

Mancanza di isolamento delle risorse

L'utilizzo di risorse da parte di un cliente può avere effetti sulle risorse di una altro cliente.

Le infrastrutture di cloud computing IaaS fanno affidamento soprattutto su design di architettura dove le risorse fisiche sono condivise da multiple macchine virtuali e quindi clienti multipli.

Vulnerabilità nell'hypervisor possono portare ad un accesso non autorizzato a queste risorse condivise. Per esempio, le macchine virtuali del Cliente 1 e del Cliente 2 hanno i loro hard drive virtuali salvati sullo stesso LUN (Logical Unit Number) condiviso dentro una Storage Area Network. Il Cliente 2 può essere in grado di mappare l'hard drive virtuale del Cliente 1 alla sua macchina virtuale e quindi vedere ed utilizzare i dati ivi contenuti.

La mancanza di strumenti per applicare dei Termini di Utilizzo o un più specifico Service Level Agreement (SLA), come Quality of Service o prodotti di distributed resource scheduling (DRS), possono permettere ad un cliente di monopolizzare l'utilizzo delle risorse, causando denial of service o scarsa performance agli altri utenti del servizio.

Mancanza di isolamento di reputazione

Si ha quando le attività di un utente impattano la reputazione di un altro utente. Questo può avvenire in un contesto di mancanza di isolamento delle risorse, perciò un attaccante riesce a manipolare a suo piacimento le risorse di altri utenti del cloud. Tuttavia difficilmente una minaccia riesce ad attaccare un bersaglio specifico in quanto i dati ai quali ha accesso in genere non sono la totalità ma solo quelli presenti in quel momento nel dispositivo di storage fisico di cui ha il controllo.

Possibilità che la rete interna venga spiata

Questo avviene quando i clienti cloud possono effettuare port scan e altri test su altri clienti sulla stessa rete interna.

Vulnerabilità di autenticazione e autorizzazione

Uno scarso sistema di autenticazione e autorizzazione può facilitare l'accesso non autorizzato a risorse, il privilege escalation, l'impossibilità di tenere sotto controllo l'uso improprio di risorse e incidenti di sicurezza, etc,

attraverso:

- Immagazzinamento non sicuro delle credenziali di accesso cloud da parte del cliente;
- Ruoli disponibili insufficienti;
- Credenziali immagazzinate su una macchina transitoria;

Inoltre il cloud rende gli attacchi a sistemi di autenticazione basati su password molto più impattanti in quanto le applicazioni delle aziende ora sono esposte su Internet. Quindi l'autenticazione basata su password diventerà insufficiente e sarà necessario un sistema di autenticazione più forte (ad esempio a due fattori).

Impossibilità di processare dati in forma criptata

Homomorphic encryption: una forma di criptazione che permette di svolgere tipi specifici di computazioni direttamente sul testo cifrato, e di ottenere un risultato criptato che corrisponde al testo cifrato del risultato dell'operazione effettuata sul testo in chiaro.
Criptare i dati staticamente non è difficile, ma nonostante i recenti progressi nella homomorphic encryption, c'è poca prospettiva che un sistema commerciale riesca a mantenere questo tipo di criptazione durante l'elaborazione. In un articolo, Bruce Schneier stima che effettuare una ricerca web utilizzando keyword criptate aumenterebbe il tempo di computazione di circa mille miliardi di volte[12]. Questo significa che per molto tempo a venire, i clienti cloud che fanno qualcosa di diverso dall'immagazzinare dati dovranno fidarsi del cloud provider.

Accesso remoto alle interfacce di gestione

Le interfacce di gestione possono essere accedute da Internet per cui tutte le vulnerabilità del canale sono da tenere in considerazione, come ad esempio attacchi del tipo man-in-the-middle, replay, spoofing della rete.

Vulnerabilità di criptazione della comunicazione

Queste vulnerabilità riguardano la possibilità di lettura dei dati in transito

tramite, ad esempio, attacchi MITM, autenticazione scarsa, accettazione di certificati auto firmati, etc. In questo senso è bene che i dati in transito siano sempre criptati.

Possibilità di controllo dei co-residenti

Attacchi di tipo side-channel che sfruttano mancanza di isolamento delle risorse permettono ad un attaccante di determinare quali risorse sono condivise da quale cliente.

Sanitization dei media sensibili

La condivisione del dispositivo fisico di memoria tra vari utenti implica che dati sensibili possono trapelare in quanto le procedure di distruzione applicabili al termine del servizio possono essere impossibili da implementare perché, ad esempio, il media non può essere fisicamente distrutto a conseguenza del fatto che un disco è ancora in uso da un altro utente.

Vulnerabilità nel provisioning dell'utente

- Il cliente non può controllare il processo di approvigionamento
- L'identità del cliente non è adeguatamente verificata in fase di registrazione
- Avvengono ritardi nella sincronizzazione tra componenti di un sistema cloud
- Vengono create copie multiple e non sincronizzate dei dati di identità
- Le credenziali sono vulnerabili ad intercettazione e replay

Nessuna regola riguardo il massimo utilizzo di risorse

Se non c'è una maniera flessibile e configurabile per il cliente o il provider per poter impostare il limite sull'utilizzo delle risorse, può essere problematico quando l'uso di una risorsa è impredicibile. In questo caso il cliente è vulnerabile ad attacchi del tipo economic denial of service, mentre il provider (e tutti i clienti che si appoggiano al provider) è vulnerabile a denial of service.

Procedure di gestione delle chiavi inadeguate

Le infrastrutture di cloud computing necessitano di gestione e memorizzazione di molti differenti tipi di chiavi; esempi includono chiavi di sessione per proteggere dati in transito (chiavi SSL), chiavi di criptazione file, coppia di chiavi che identificano il provider, coppia di chiavi che identificano il cliente e token di autorizzazione. Visto che le virtual machine non hanno una infrastruttura hardware fissa e il contenuto di un cloud tende ad essere geograficamente distribuito, è più difficile applicare controlli standard, come memorizzazione in hardware security module (HSM), alle chiavi in una infrastruttura cloud.[13]

Gli HSM sono per necessità fortemente protetti fisicamente. Questo rende molto difficile distribuirli nelle multiple posizioni usate nelle architetture cloud. Inoltre le interfacce di gestione delle chiavi che sono accessibili tramite Internet pubblico sono più vulnerabili, visto che la sicurezza è diminuita dal canale di comunicazione tra l'utente e lo storage di chiave cloud.

Generazione delle chiavi: entropia bassa per la generazione di numeri casuali

La combinazione di immagini di sistema standard, tecnologie di virtualizzazione e mancanza di device di input porta il sistema ad avere entropia molto più bassa rispetto ai generatori di numeri random hardware. Questo significa che un attaccante su una macchina virtuale può essere in grado di indovinare le chiavi di criptazione generate su altre macchine virtuali perché le sorgenti di entropia sono simili. Non è un problema difficile da risolvere di per sè, ma se non è considerato a tempo di design può avere importanti conseguenze.

Immagazzinamento di dati in multiple giurisdizioni e mancanza di trasparenza a riguardo

La memorizzazione dei dati ridondante senza disponibilità per il cliente di informazioni in tempo reale riguardo la posizione dei dati introduce un livello di vulnerabilità. Le compagnie potrebbero inavvertitamente violare regolamenti, specialmente se non sono disponibili informazioni chiare ri-

guardo la giurisdizione dello storage.

Mancanza di informazioni riguardo giurisdizioni

I dati potrebbero essere immagazzinati e/o processati in giurisdizioni ad alto rischio dove sono vulnerabili a confisca tramite effrazione. Se questa informazione non è disponibile al cliente, esso non può prendere le precauzioni necessarie per evitare il danno.

Ruoli e responsabilità non chiari
Principio Need-to-know non applicato
Applicazione inadeguata delle definizioni dei ruoli

Queste vulnerabilità riguardano la suddivisione in ruoli e la definizione di responsabilità di tali ruoli. Se a un ruolo vengono dati meno privilegi di quanti ne siano necessari allo svolgimento delle funzioni di tale ruolo esiste un problema. Se, in modo complementare, vengono dati troppi privilegi a un ruolo si possono creare grosse falle nell'organizzazione del provider.[2]

Mancanza di security awareness

I clienti cloud possono non essere consapevoli dei rischi che corrono migrando al cloud, in particolare i rischi generati da minacce specifiche del cloud, quali perdita di controllo, lock-in del venditore, risorse del cloud provider esaurite, etc. Questa mancanza di consapevolezza può anche influenzare il cloud provider, che può non essere al corrente delle azioni da intraprendere per mitigare questi rischi.

2.3 Analisi di rischio in ambiente Cloud

Notare i seguenti punti in relazione alle sezioni successive:

- I rischi devono essere sempre considerati in relazione all'opportunità di business complessiva - a volte un rischio è compensato da una opportunità.
- Il livello di rischio in molti casi varia significativamente a seconda del tipo di architettura cloud considerata.

- Può capitare che il cliente cloud trasferisca il rischio al provider cloud e il rischio deve essere considerato rispetto ai benefici economici ricevuti dal provvedere questi servizi. Tuttavia non tutti i rischi possono essere trasferiti: se un rischio porta al fallimento di un business, danni seri alla reputazione o implicazioni legali, è difficile o impossibile far compensare questo danno a terzi.
- L'analisi di rischio è espressa dal punto di vista del cliente cloud.

2.3.1 Rischi organizzativi e di policy

2.3.1.1 Lock-in

Probabilità	ALTA
Impatto	MEDIO
Vulnerabilità	Mancanza di tecnologie e soluzioni standard Poca scelta di provider Mancanza di completezza e trasparenza nei termini di utilizzo
Beni afflitti	Reputazione dell'azienda Dati personali sensibili Service delivery
Rischio	ALTO

Il vendor lock-in consiste nel rendere il cliente dipendente ad un particolare venditore in quanto a prodotti e servizi, inabile nel poter cambiare venditore senza costi di migrazione sostanziali.
Correntemente l'offerta di strumenti, procedure, formati di dato standard o interfacce di servizio che possono garantire portabilità di dati e servizi è praticamente nulla. Questo rende la migrazione da un provider ad un altro estremamente difficile; in più, i provider possono essere incentivati ad impedire la portabilità dei servizi e dei dati dei propri clienti.
Questa potenziale dipendenza ad un particolare provider, a seconda degli impegni del provider, possono portare a disastri di business catastrofici se il provider dovesse andare in bancarotta e il costo per la migrazione del servizio e dei dati dovesse essere troppo alto.
L'acquisizione del cloud provider da parte di altre aziende può avere un effetto simile, visto che questo aumenta la probabilità di cambiamenti improvvisi nelle politiche del provider o nei termini di utilizzo.[7]

2.3.1.2 Perdita di controllo

Probabilità	MOLTO ALTA
Impatto	IaaS MOLTO ALTO SaaS BASSO
Vulnerabilità	Ruoli e responsabilità non chiari Applicazione inadeguata delle definizioni di ruoli Clausole nel SLA con promesse in conflitto per diversi portatori di interesse Revisioni e certificazioni non disponibili ai clienti Mancanza di tecnologie e soluzioni standard Mancanza di informazioni riguardo giurisdizioni Mancanza di completezza e trasparenza nei termini di utilizzo Proprietà dei beni incerta
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Dati personali sensibili Service delivery
Rischio	ALTO

Utilizzando infrastrutture cloud, il cliente cede necessariamente il controllo al provider cloud riguardo un numero di questioni che possono influenzare la sicurezza. Per esempio i termini di utilizzo possono proibire scan delle porte, valutazione delle vulnerabilità e penetration testing. Inoltre ci possono essere conflitti tra le procedure di hardening del cliente e l'ambiente cloud. Il Service Level Agreement può non offrire impegno da parte del provider a provvedere questi servizi, lasciando un gap nelle difese.[11]

In più il provider stesso può dare servizi in outsourcing a compagnie terze che non offrono le stesse garanzie del provider.

2.3.1.3 Problemi di conformità

Probabilità	MOLTO ALTA
Impatto	ALTO
Vulnerabilità	Revisioni e certificazioni non disponibili ai clienti Mancanza di tecnologie e soluzioni standard Mancanza di completezza e trasparenza nei termini di utilizzo
Beni afflitti	Certificazione
Rischio	ALTO

Certe organizzazioni migrando al cloud hanno investito considerevolmente nell'ottenere certificazioni per soddisfare lo standard dell'industria o per requisiti di regolamento. Questo investimento può essere messo a rischio migrando al cloud in quanto:

- Il cloud provider può non fornire prova riguardo la sua conformità al requisito rilevante
- il cloud provider può non permettere verifiche da parte del cliente

In alcuni casi, questo significa che utilizzare una infrastruttura cloud pubblica implica che certi tipi di conformità non possono essere ottenute e quindi i servizi ospitati nel cloud non possono essere utilizzati per servizi che necessitano tali conformità.

2.3.1.4 Perdita di reputazione a causa delle attività di co-tenant

Probabilità	BASSA
Impatto	ALTO
Vulnerabilità	Mancanza di isolamento delle risorse Mancanza di isolamento di reputazione Vulnerabilità dell'hypervisor
Beni afflitti	Reputazione dell'azienda Dati personali sensibili Service delivery
Rischio	MEDIO

La condivisione di risorse fa si che attività dolose da parte di un tenant

possano influenzare la reputazione di un altro tenant. Per esempio, spamming, port scanning o servire contenuto malevolo dalla infrastruttura può portare a:

- un range di indirizzi IP bloccati, inclusi quello dell'attaccante e di altri tennat innocenti
- confisca delle risorse a causa di attività di altri tenant

L'impatto può essere discontinuità nel service delivery, perdite di dati e problemi alla reputazione dell'azienda.

2.3.1.5 Supply chain failure

Probabilità	BASSO
Impatto	MEDIO
Vulnerabilità	Mancanza di completezza e trasparenza nei termini di utilizzo Dipendenze nascoste create da applicazioni cross-cloud Poca scelta di provider
Beni afflitti	Reputazione dell'azienda Affidabilità verso il cliente Dati personali sensibili Service delivery
Rischio	MEDIO

Un provider cloud può dare in outsource alcuni compiti specializzati nella sua catena di produzione. In questa situazione il livello di sicurezza del cloud provider dipende dal livello di sicurezza di ogni azienda su cui fa outsource. Qualunque interruzione o corruzione della catena o mancanza di coordinazione delle responsabilità tra tutti i membri coinvolti può portare a: interruzione del servizio, perdita di dati, confidenzialità, integrità e availability, perdite econimiche e di reputazione, violazione di SLA etc.

In generale, la mancanza di trasparenza nel contratto può essere un problema per tutto il sistema. Se il provider non dichiara quali servizi core sono in outsourcing il cliente non è in grado di valutare opportunamente i rischi che corre.

2.3.2 Rischi che riguardano aspetti tecnologici e architetturali

2.3.2.1 Esaurimento delle risorse (sotto o sovra approvigionamento)

Probabilità	Inabilità a fornire capacità addizionale all'utente: MEDIA Inabilità a fornire capacità correntemente accordata: BASSA
Impatto	Inabilità a fornire capacità addizionale all'utente: BASSO Inabilità a fornire capacità correntemente accordata: ALTO
Vulnerabilità	Modellazione inaccurata dell'utilizzo delle risorse Inadeguato approvvigionamento delle risorse ed investimento in infrastrutture Nessuna regola riguardo il massimo utilizzo di risorse
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Service delivery
Rischio	MEDIO

I servizi cloud sono servizi on-demand. Per questo c'è un livello di rischio calcolato nell'allocare tutte le risorse di un servizio cloud, perché le risorse sono allocate secondo delle proiezioni statistiche.[3] Modellazione inaccurata dell'utilizzo delle risorse o approvvigionamento inadeguato e investimenti nelle infrastrutture inadeguati possono portare, dal punto di vista del cloud provider, a:

- Service unavailability: fallimenti in certi scenari applicativi molto specifici, in cui una risorsa viene utilizzata molto intensamente;
- Perdite economiche e reputazionali: a causa del fallimento nel soddisfare le richieste del cliente
- Sovradimensione dell'infrastruttura: approvvigionamento eccessivo può portare a perdite economiche e di redditività

2.3.2.2 Isolation failure

Probabilità	BASSA (Cloud privata) MEDIA (Cloud pubblica)
Impatto	MOLTO ALTO
Vulnerabilità	Vulnerabilità dell'hypervisor Mancanza di isolamento delle risorse Mancanza di isolamento di reputazione Possibilità che la rete interna venga spiata
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Dati personali, anche sensibili Service delivery
Rischio	ALTO

Il multi-tenancy e le risorse condivise sono due delle caratteristiche che definiscono l'ambiente cloud. Capacità di computazione, memorizzazione e rete sono condivise tra diversi utenti. Questa classe di rischi include il fallimento di meccanismi che si occupano di separare i dati, la memoria e anche la reputazione tra diversi utenti dell'infrastruttura condivisa (esempio con attacchi guest-hopping, sql injection su una tabella contenente dati di più clienti, attacchi side-channel).

La probabilità di questo scenario dipende dal modello di cloud considerato; sarà basso in un cloud privato e più alto in cloud pubblico.

L'impatto può essere perdita di dati sensibili, perdita di reputazione e interruzione di servizio sia per i provider che per i clienti.

2.3.2.3 Malicious insider - abuso di ruoli privilegiati

Probabilità	MEDIA
Impatto	MOLTO ALTO
Vulnerabilità	Ruoli e responsabilità non chiari Applicazione inadeguata delle definizioni dei ruoli Principio Need-to-know non applicato Vulnerabilità di autenticazione e autorizzazione Vulnerabilità di sistema Procedure di sicurezza fisica inadeguate Impossiblità di processare dati in forma criptata Vulnerabilità di applicazione / patch management inadeguato
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Proprietà intellettuale del cliente Dati sensibili Service delivery
Rischio	ALTO

Un insider è un individuo all'interno dell'azienda spesso con ruoli di accesso privilegiati che va contro gli interessi dell'azienda, ad esempio rubando dati o manomettendo il sistema. Le attività di un insider possono potenzialmente avere impatto su: confidenzialità, integrità e disponibilità di tutti i tipi di dato, proprietà intellettuale, reputazione dell'azienda e affidabilità dell'azienda rispetto ai clienti. Man mano che il cloud viene sempre più utilizzato, gli impiegati di cloud provider diventano bersaglio di atti criminali (come è stato testimoniato nell'industria dei servizi finanziari con gli impiegati di call centre [5]).

2.3.2.4 Compromissione di interfacce di gestione

Probabilità	MEDIA
Impatto	MOLTO ALTO
Vulnerabilità	Vulnerabilità di autenticazione e autorizzazione Accesso remoto alle interfacce di gestione Vulnerabilità di sistema Vulnerabilità di applicazione / patch management inadeguato
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Dati sensibili Service delivery Interfacce di gestione del servizio
Rischio	MEDIO

Le interfacce di gestione del servizio cloud per il cliente sono accessibili via Internet e mediano l'accesso ad un insieme di risorse più grande rispetto ai tradizionali servizi di hosting, quindi pongono un rischio aumentato, specialmente se combinato con vulnerabilità di accesso remoto e del web browser. Questo include interfacce di clienti che controllano un numero alto di virtual machine, ma soprattutto le interfacce del cloud provider che controllano l'intero sistema cloud.

2.3.2.5 Intercettazione dati in transito

Probabilità	MEDIA
Impatto	ALTO
Vulnerabilità	Vulnerabilità di autenticazione e autorizzazione Vulnerabilità di criptazione della comunicazione Possibilità che la rete interna venga spiata Possibilità di controllo dei co-residenti
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Proprietà intellettuale Dati sensibili
Rischio	MEDIO

Il cloud computing, in quanto architettura distribuita, implica più dati in

transito rispetto alle normali infrastrutture. Per esempio vengono trasferiti dati per sincronizzare più immagini distribuite, tra infrastrutture cloud e client remoti, etc. In più, molti dei servizi di hosting di dati sono implementati utilizzando un ambiente vpn-like sicuro, una pratica non sempre seguita in contesto cloud.

Sniffing, spoofing, attacchi man-in-the-middle e attacchi replay sono da considerare possibili fonti di minaccia.

Inoltre in alcuni casi il cloud provider non offre confidenzialità o condizioni di non-disclosure o queste condizioni non sono sufficienti a garantire rispetto per la protezione delle informazioni segrete del cliente.[8]

2.3.2.6 Cancellazione dei dati insicura o inefficace

Probabilità	MEDIO
Impatto	MOLTO ALTO
Vulnerabilità	Sanitization dei media sensibili
Beni afflitti	Dai personali Dati sensibili Credenziali
Rischio	MEDIO

Quando un cliente termina la richiesta di servizio, le risorse sono ridimensionate, l'hardware viene riallocato, etc, e i dati possono essere disponibili oltre il tempo specificato nel contratto di sicurezza. Può essere impossibile applicare le procedure di eliminazione specificate nel contratto di sicurezza, visto che la cancellazione totale dei dati è possibile soltanto distruggendo il disco che contiene anche i dati di altri clienti. Quando viene effettuata una richiesta di cancellazione di una risorsa cloud, questo potrebbe non risultare nella cancellazione vera dei dati. Quando è necessaria la vera eliminazione dei dati devono essere seguite procedure speciali e questo potrebbe non essere supportato dalle API standard (o potrebbe non essere supportato affatto).

Se viene utilizzata criptazione si può considerare più basso il livello di rischio.

2.3.2.7 Distributed denial of service

Probabilità	Cliente: MEDIA Provider: BASSA
Impatto	Cliente: MEDIO Provider: MOLTO ALTO
Vulnerabilità	Errori di configurazione Vulnerabilità di sistema Risorse di filtraggio inadeguate o configurate erroneamente
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Service delivery Interfacce di gestione del servizio Rete (connessioni etc)
Rischio	MEDIO

2.3.2.8 Economic denial of service

Probabilità	BASSA
Impatto	ALTO
Vulnerabilità	Vulnerabilità di autenticazione e autorizzazione Vulnerabilità nel provisioning dell'utente Vulnerabilità nel de-provisioning dell'utente Accesso remoto a interfacce di gestione Nessuna regola riguardo il massimo utilizzo di risorse
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Service delivery Risorse monetarie del cliente
Rischio	MEDIO

L'economic denial of service è un rischio nato con il cloud computing, in particolare per la sua natura pay-per-use. In un attacco EDoS lo scopo è di rendere il modello di fatturazione cloud insostenibile e quindi impedire che una compagnia riesca a utilizzare o pagare l'infrastruttura cloud. Consiste nello sfruttare vulnerabilità nel sistema di fatturazione per far sem-

brare legittimo l'utilizzo malevolo del servizio mentre alza i costi a livello ingestibile.

Ci sono differenti scenari in cui le risorse del cliente possono essere usate per aver un impatto economico:

- Furto d'identità: un attaccante sfrutta un account per utilizzare le risorse del cliente (la vittima) per il proprio vantaggio o per danneggiare economicamente la vittima

- Il cliente cloud non ha impostato limiti all'utilizzo delle risorse per cui paga e sperimenta carichi inaspettati su queste risorse tramite nessuna azione dolosa

- Un attaccante usa un canale pubblico per utilizzare le risorse per cui il cliente paga - ad esempio, se un cliente paga per ogni richiesta HTTP ricevuta, un attacco DDoS può avere anche l'effetto di EDoS

Gli attacchi EDoS distruggono le risorse economiche; il worst case scenario sarebbe la bancarotta del cliente o un impatto economico serio.

2.3.2.9 Perdita di chiavi di criptazione

Probabilità	BASSA
Impatto	ALTO
Vulnerabilità	Procedure di gestione delle chiavi inadeguate Generazione delle chiavi: entropia bassa per la generazione di numeri casuali
Beni afflitti	Proprietà intellettuale Dati personali sensibili Credenziali
Rischio	MEDIO

Include la divulgazione di chiavi segrete (SSL, chiavi di criptazione file, chiavi private del cliente, etc), la perdita o corruzione di dette chiavi, o il loro uso non autorizzato per l'autenticazione o la non-ripudiazione (firma digitale).

2.3.2.10 Scan e probe malevoli

Probabilità	MEDIA
Impatto	MEDIO
Vulnerabilità	Possibilità che la rete interna venga spiata Possibilità di controllo dei co-residenti
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Service delivery
Rischio	MEDIO

Scan e probe malevoli, così come il mapping della rete, sono minacce indirette ai beni considerati. Possono essere utilizzati per raccogliere informazioni nel contesto di un tentativo di hack. Un possibile impatto può essere perdita di confidenzialità, integrità e disponibilità di servizi e dati.

2.3.2.11 Compromissione del service engine

Probabilità	BASSA
Impatto	MOLTO ALTO
Vulnerabilità	Vulnerabilità dell'hypervisor Mancanza di isolamento delle risorse
Beni afflitti	Dati personali sensibili Service delivery
Rischio	MEDIO

Ogni architettura cloud si basa su una piattaforma altamente specializzata, il service engine, che giace sopra le risorse fisiche hardware e gestisce le risorse del cliente a diversi livelli di astrazione. Per esempio, nei cloud IaaS questo componente può essere l'hypervisor. Il service engine è sviluppato e supportato dai venditori di piattaforme cloud e in alcuni casi dalla community open source. Può essere ulteriormente personalizzato dai provider di cloud computing.

Come ogni altro layer software, il codice del service engine può avere vulnerabilità ed è soggetto ad attacchi o failure inaspettati. Un attaccante può compromettere il service engine manomettendolo da dentro una macchina virtuale (cloud IaaS), dall'ambiente di runtime (PaaS), dall'applicazione (SaaS), o tramite le sue API.

Manomettere il service engine può essere utile per uscire dall'isolamento degli environment di diversi clienti o per acquisire l'accesso a dati ivi contenuti, per monitorarne e modificarne le informazioni contenute in maniera trasparente (senza interazione diretta con l'applicazione dentro l'environment del cliente), o per ridurre le risorse assegnate ad un cliente, causandone denial of service.

2.3.2.12 Conflitti tra procedure di hardening del cliente ed environment cloud

Probabilità	BASSA
Impatto	MEDIO
Vulnerabilità	Mancanza di completezza e trasparenza nei termini di utilizzo Clausole nel SLA con promesse in conflitto per diversi portatori di interesse Ruoli e responsabilità non chiari
Beni afflitti	Proprietà intellettuale Dati personali sensibili
Rischio	MEDIO

I cloud provider devono impostare chiaramente una segregazione delle responsabilità che articola le azioni minime che un cliente deve intraprendere. Il fallimento da parte del cliente di rendere sicuro il proprio environment può costituire una vulnerabilità alla piattaforma cloud se il cloud provider non ha isolato accuratamente il sistema. I cloud provider dovrebbero articolare ulteriormente i loro meccanismi di isolamento e provvedere delle linee guida per assistere i loro clienti a rendere sicure le loro risorse.

I clienti devono assumersi le loro responsabilità in quanto se non lo fanno porrebbero i loro dati e le loro risorse ad un ulteriore rischio. In alcuni casi i clienti cloud hanno inappropriatamente dato per scontato che il cloud provider fosse responsabile per tutte le attività necessarie a rendere sicuri i propri dati. Questa assunzione da parte del cliente, e/o mancanza da parte del provider di una chiara articolazione, mette sotto rischio i dati del cliente. E' imperativo che il cliente cloud identifichi le proprie responsabilità e che le soddisfi.

I cloud provider, per loro natura, devono provvedere un ambiente multi-tenant; la co-locazione di molti clienti causa inevitabilmente conflitti per il cloud provider in quanto i requisiti di sicurezza per la comunicazione di ogni cliente cloud probabilmente differiscono da utente ad utente. Si prenda, ad esempio, il caso di due clienti su una infrastruttura tradizionale di rete condivisa. Se un cliente vuole che il firewall di rete blocchi tutto il traffico eccetto SSH, mentre un altro cliente sta eseguendo un web server e necessita il passaggio di HTTP e HTTPS, chi vince? Lo stesso tipo di problema si verifica per clienti che hanno requisiti conflittuali. Questo tipo di sfida peggiora mano a mano che i clienti e la disparità dei loro requisiti aumenta. Perciò i cloud provider devono essere in una posizione che permette loro di trattare queste sfide tramite tecnologia, policy e trasparenza.

2.3.3 Rischi legali

2.3.3.1 Sub poena

Probabilità	ALTA
Impatto	MEDIO
Vulnerabilità	Mancanza di isolamento delle risorse Immagazzinamento di dati in multiple giurisdizioni e mancanza di trasparenza a riguardo Mancanza di informazioni riguardo giurisdizioni
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Dati personali sensibili Service delivery
Rischio	ALTO

Sub poena è una espressione di origine latina per designare il diritto di un organismo statuale (in genere un giudice) di costringere la testimonianza di un teste o la produzione di elementi di prova con l'avviso che il mancato rispetto comporta una sanzione.
Nell'evento di confisca di hardware fisico come risultato di sub poena, la centralizzazione della memoria assieme alla tenancy condivisa dell'hardware fisico pone molti clienti a rischio di divulgazione dei propri dati a terzi.

Contemporaneamente, può essere impossibile per una agenzia di una singola nazione confiscare un cloud dati i progressi riguardo la migrazione a lunga distanza di macchine virtuali da parte di un hypervisor.

2.3.3.2 Rischi derivanti dai cambi giurisdizionali

Probabilità	MOLTO ALTA
Impatto	ALTO
Vulnerabilità	Mancanza di informazioni riguardo giurisdizioni Immagazzinamento di dati in multiple giurisdizioni e mancanza di trasparenza a riguardo
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Dati personali sensibili Service delivery
Rischio	ALTO

I dati dei clienti potrebbero residuare in multiple giurisdizioni, alcune delle quali potrebbero essere un rischio. Se i centri dei dati sono localizzati in paesi ad alto rischio, esempio quelli la cui struttura legislativa risulta imprevedibile, stati di polizia autocratici, stati che non rispettano gli accordi internazionali etc, i dati possono essere divulgati o confiscati dalle autorità locali.

2.3.3.3 Rischi di protezione dati

Probabilità	ALTA
Impatto	ALTO
Vulnerabilità	Mancanza di informazioni riguardo giurisdizioni Immagazzinamento di dati in multiple giurisdizioni e mancanza di trasparenza a riguardo
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Dati personali sensibili Service delivery
Rischio	ALTO

Il cloud computing pone diversi rischi per la protezione dei dati per i client cloud e per i provider.

- Può essere difficile per il cliente tenere sotto controllo l'elaborazione dei dati da parte del provider, e quindi essere sicuro che i dati siano gestiti in maniera legale. Deve essere chiaro che il cliente cloud sarà il principale responsabile per l'elaborazione dei dati personali, anche quando questa elaborazione viene effettuata da parte del provider cloud. Fallimenti nel rispettare le leggi di protezione dei dati può portare a sanzioni di tipo amministrativo, civile o addirittura penale. D'altra parte alcuni cloud provider forniscono informazioni in tal senso, provvedendo riassunti riguardo le elaborazioni dei dati che hanno effettuato, le loro attività di security sui dati e i controlli che praticano.

- Ci possono essere brecce di sicurezza che non sono notificate al controllore (il cliente) da parte del provider.

- Il cliente potrebbe perdere il controllo dei dati elaborati dal provider. Il problema è aumentato in caso di multipli trasferimenti di dati (esempio tra cloud provider fedarati).

- Il cloud provider può ricevere dati che non sono stati ottenuti legalmente da parte del cliente.

2.3.3.4 Rischi riguardanti le licenze

Probabilità	MEDIA
Impatto	MEDIO
Vulnerabilità	Mancanza di completezza e trasparenza nei termini di utilizzo
Beni afflitti	Reputazione dell'azienda Service delivery Certificazione
Rischio	MEDIO

Condizioni di licenza, come agreement per-seat e controlli di licenza online possono diventare inapplicabili in un ambiente cloud. Per esempio, se il software è addebitato per ogni istanza ogni volta che una nuova macchina è istanziata allora i costi di licenza dell'utente cloud può aumentare esponenzialmente anche se usa lo stesso numero di istanze di macchine per la stessa durata.

2.3.4 Rischi non specifici al cloud

In questa sezione verrà elencata una serie di minacce non specifiche al cloud ma che vanno comunque considerate attentamente quando si valutano i rischi di un tipico sistema cloud.

2.3.4.1 Rottura della rete

Probabilità	BASSA
Impatto	MOLTO ALTO
Vulnerabilità	Errori di configurazione Vulnerabilità del sistema o dell'OS Mancanza di isolamento delle risorse Mancanza o inadeguatezza di un disaster recovery plan
Beni afflitti	Service delivery
Rischio	MEDIO

Uno dei rischi più grandi. Potenzialmente migliaia di utenti ne sono influenzati contemporaneamente.

2.3.4.2 Gestione di rete (congestione di rete / errori di configurazione / uso non ottimale)

Probabilità	MEDIA
Impatto	MOLTO ALTO
Vulnerabilità	Errori di configurazione Vulnerabilità del sistema o dell'OS Mancanza di isolamento delle risorse Mancanza o inadeguatezza di un disaster recovery plan
Beni afflitti	Reputazione dell'azienda Affidabilità verso i clienti Service delivery Rete (connessioni, etc)
Rischio	ALTO

2.3.4.3 Privilege escalation

Probabilità	BASSA
Impatto	ALTO
Vulnerabilità	Vulnerabilità di autenticazione e autorizzazione Vulnerabilità nel provisioning dell'utente Vulnerabilità nel de-provisioning dell'utente Vulnerabilità dell'hypervisor Ruoli e responsabilità non chiari Applicazione inadeguata delle definizioni dei ruoli Errori di configurazione
Beni afflitti	Dati personali sensibili Controllo di accesso Directory utente (dati)
Rischio	MEDIO

2.3.4.4 Attacchi di social engineering

Probabilità	MEDIA
Impatto	ALTA
Vulnerabilità	Mancanza di security awareness Vulnerabilità nel provisioning dell'utente Mancanza di isolamento delle risorse Vulnerabilità di criptazione della comunicazione Procedure di sicurezza fisica inadeguate
Beni afflitti	Reputazione dell'azienda Affidabilità verso il cliente Proprietà intellettuale Dati personali sensibili Controllo di accesso Credenziali
Rischio	MEDIO

2.3.4.5 Accesso non autorizzato agli edifici aziendali (incluso accesso fisico alle macchine)

Probabilità	MOTLO BASSA
Impatto	ALTO
Vulnerabilità	Procedure di sicurezza fisica inadeguate
Beni afflitti	Reputazione dell'azienda Affidabilità verso il cliente Dati personali sensibili Backup o dati archiviati
Rischio	MEDIO

Visto che i cloud provider concentrano le risorse in diversi data centre, anche se i controlli del perimetro fisico sono probabilmente più forti del normale, l'impatto di una breccia in quei controlli è più alta in quanto la sicurezza dei dati di tutti i clienti le cui risorse sono memorizzate in quel centro di dati è compromessa.

Capitolo 3

Cloud Network Security Framework

Il cloud computing porta con sè una gamma talmente ampia di rischi che considerare una soluzione integrata è impossibile. Ciò che si può fare è lavorare su singoli o gruppi molto legati di fattori di rischio (vulnerabilità) cercando di risolvere problemi con aspetti condivisi.
Di seguito verrà discusso un framework per il cloud security che si occupa di risolvere il problema di intrusione nella rete cloud.

In questo framework, proposto da Modi, Patel, Borisanya, Patel e Rajarajan al 5th International Conference on Security of Information and Networks, viene proposto di integrare un network intrusion detection system (NIDS) nella infrastruttura cloud. Viene utilizzato snort e un decision tree classifier per rilevare gli attacchi nella rete, mentre viene mantenuta la performance e la qualità del servizio.

L'obiettivo del framework è quello di rilevare intrusi in reti tradizionali e virtuali nel cloud, e di ridurre i falsi allarmi con costo computazionale abbordabile.

3.1 Background teorico

3.1.1 Snort

Per il rilevamento basato su signature viene utilizzato Snort, un packet sniffer e NIDS molto conosciuto ed open source. E' configurabile, gratuito, può essere eseguito su diversi tipi di piattaforme ed è costantemente mantenuto aggiornato. Snort cattura i pacchetti di dati nella rete e controlla il loro contenuto confrontandoli con pattern predefiniti alla ricerca di correlazioni. Il detection engine di Snort permette di registrare, allertare e rispondere ad ogni attacco conosciuto. L'unico problema è che Snort non può rilevare attacchi sconosciuti. Per questo viene utilizzato un decision tree classifier, un approccio proprio del machine learning.

3.1.2 Decision Tree Classifier

Per il rilevamento di anomalie, viene utilizzata una tecnica di DT Classifier, che costruisce una struttura ad albero dalla cima alla base. Nell'albero generato ogni nodo rappresenta il nome della caratteristica del pacchetto, ogni foglia indica la classe e ogni ramo rappresenta un risultato (o valore) del nodo associato. Dopo aver generato l'albero, vengono definite regole tracciando ogni percorso dalla radice alle foglie. I DT possono classificare grandi quantità di dati con velocità di apprendimento più alta rispetto ad altre tecniche di classificazione e ha una precisione di rilevamento più alta. In questo approccio viene utilizzato l'algoritmo ID3, costruendo l'albero decisionale in questo modo:
Input: Training set di pacchetti D.
Output: Albero decisionale T.
Step 1:

- Se tutti i pacchetti nel dataset D sono normali, crea un nodo "Normal" e si ferma.
- Se tutti i pacchetti nel dataset D sono intrusioni, crea un nodo "Intrusion" e si ferma.

- Altrimenti sceglie una caratteristica F con valori f_1, f_2,... f_n, e crea un nodo decisionale.

Step 2:
Partiziona i training packets in D in sottoinsiemi D_1, D_2,...,D_n a seconda dei valori di F.
Step 3:
Applica l'algoritmo ricorsivamente per ogni insieme D_i.

Per scegliere le caratteristiche su cui fare split nell'albero decisionale, viene calcolato il guadagno informativo per ogni caratteristica. Quindi viene scelta la caratteristica con maggior guadagno informativo. Il guadagno informativo per ogni attributo è derivato dalle equazioni 3.1, 3.2 e 3.3.

$$Info(D) = -\sum_{i=1}^{m} P_i \times \log_2(P_i) \tag{3.1}$$

Dove m è il numero di classi, P_i la probabilità che un pacchetto in D appartenga alla classe C_i, calcolato da $|C_i, D|/|D|$.

$$Info\_F(D) = -\sum_{j=1}^{v}(|D_j|/|D|) \times Info(D_j). \tag{3.2}$$

$$Gain(F) = Info(D) - Info\_F(D). \tag{3.3}$$

L'equazione 3.2 indica l'informazione necessaria dopo aver utilizzato F per dividere D in v parti, mentre l'equazione 3.3 rappresenta l'informazione guadagnata effettuando branching sulla caratteristica F.
Dopo aver costruito l'albero T, vengono generate delle regole nella forma IF_THEN_ELSE tracciando ogni percorso dalla radice alle foglie. Per esempio, un percorso ha nodi (F1, F2, F3, F4) e foglia C_i allora la regola derivata è: IF F1.value=f_1 AND F2.value=f_2 AND F3.value=f_3 AND F4.value=f_4 THEN C_i. Perciò vengono generate regole per ogni percorso nell'albero, che sono poi utilizzate per classificare le class label di pacchetti di test sconosciuti.

3.2 NIDS framework per il cloud

3.2.1 Obiettivi di design

- Rilevamento di intrusioni in una rete cloud
- Basso numero di falsi positivi e falsi negativi
- Alta precisione
- Costo computazionale basso e velocità di rilevamento alta
- Scalabilità
- Compatibilità

3.2.2 Integrazione del NIDS nel cloud

I servizi cloud computing, in quanto web service, possono essere visti come composti da due parti: il front-end (lato user) e il back-end (lato server). Gli utenti cloud sono in grado di comunicare con il cloud tramite front-end, accedendo così indirettamente alla rete interna. La rete interna è

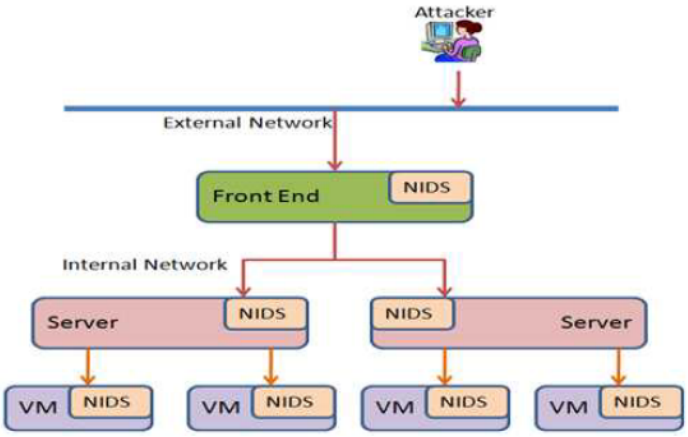


Figura 3.1: Possibli integrazioni del NIDS nel cloud.

progettata per l'interconnettività tra macchine virtuali. Nel cloud Amazon, ad esempio, le macchine virtuali hanno due IP, uno pubblico e uno privato. Le MV possono comunicare direttamente utilizzando la rete privata, mentre il NAT mappa l'ip pubblico della MV a quello privato.
Ci sono diversi livelli a cui il NIDS può lavorare nel cloud: sul front-end, sul back-end e su ogni singola macchina virtuale. Ci sono pro e contro riguardo ad ogni scelta:

- Integrare il NIDS nel front-end aiuta a rilevare intrusioni dalla rete esterna, ma non si è in grado di rilevare attacchi dalla rete interna.
- Posizionare il NIDS a livello di back-end aiuta il rilevamento di intrusi nella rete interna del cloud rilevando allo stesso tempo anche quelli nella rete esterna.
- Integrare il modulo NIDS su ogni macchina virtuale aiuta l'utente a rilevare l'intrusione sulla sua macchina virtuale. Tale configurazione necessita di multiple istanze del NIDS, rendendo la gestione dei NIDS complessa poiché le macchine virtuali possono migrare dinamicamente.

3.2.3 Architettura del modulo NIDS

Il modulo NIDS consiste in quattro parti principali: packet preprocessing, intrusion detection (composto da signature based detection e anomaly detecion), memoria (knowledge base, behavior base e central log) e sistema di allarme.

Il modulo di packet preprocessing si occupa di rimuovere informazioni ridondanti che non hanno alcuna relazione con il rilevamento.

Il modulo di intrusion detection consiste in Snort e nel Decision Tree Classifier. Snort è utilizzato per rilevare attacchi conosciuti correlando i pacchetti catturati con regole presenti nella knowledge base. Il DT Classifier costruisce un albero decisionale utilizzando la behavior base e stabilisce le class label dei pacchetti.

La memoria consiste in tre database. Il knowledge base immagazzina le signature di attacco conosciute, mentre il behavior base contiene i comportamenti considerati dannosi e quelli normali. Il central log è utilizzato per registrare eventi considerati dannosi da Snort o dal DT classifier. I moduli

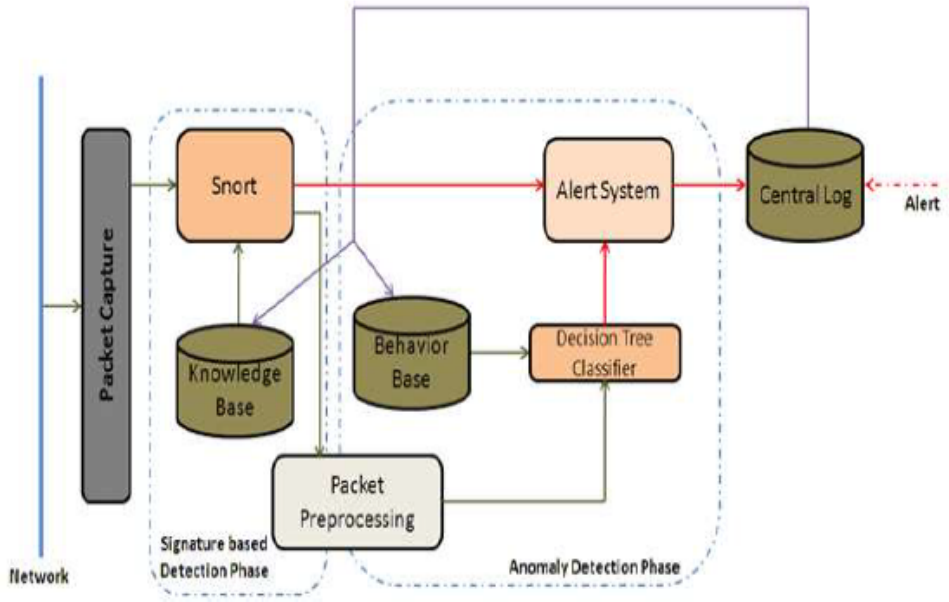


Figura 3.2: Architettura del modulo NIDS

NIDS impiegati su altri server possono aggiornare la loro knowledge base e behavior base in corrispondenza di un aggiornamento del central log.

L'alert system è utilizzato per generare un allarme in caso di anomalie rilevate da Snort o dal DT Classifier.

Nell'approccio considerato il NIDS osserva pacchetti sia dalla rete interna che dalla rete esterna. Snort confronta i pacchetti catturati con le regole presenti nel knowledge base. Se viene trovata una correlazione, viene generato un allarme che viene inviato al central log, dopodiché il pacchetto viene scartato. I pacchetti normali vengono applicati al DT classifier che determina le class label per tali pacchetti. Se il DT classifier trova intrusioni verrà generato un allarme che verrà inviato al central log, altrimenti i pacchetti vengono considerati eventi normali.

La combinazione di rilevamento signature based e behavior based aumenta la precisione di rilevamento del sistema; inoltre il metodo signature based è applicato prima di quello behavior based, riducendo i costi computazionali.

I NIDS installati su tutti i server che si basano sullo stesso central log aggiornano la loro behavior e knowledge base ogni volta che un allarme viene memorizzato nel central log: in questo modo un attacco svolto su più server contemporaneamente potrà essere velocemente rilevato su tutti i server da Snort.

Di seguito un esempio che dimostra il funzionamento del DT Classifier utilizzando un dataset esemplificativo.

Tabella 3.1: Dataset campione

ID	Protocol Type	Service	Flag	Land	Class
1	TCP	HTTP	S1	0	Normale
2	TCP	HTTP	S1	1	Normale
3	UDP	HTTP	S1	0	Intrusione
4	ICMP	SMTP	S1	0	Intrusione
5	ICMP	FTP	S0	0	Intrusione
6	ICMP	FTP	S0	1	Normale
7	UDP	FTP	S0	1	Intrusione
8	TCP	SMTP	S1	0	Normale
9	TCP	FTP	S0	0	Intrusione
10	ICMP	SMTP	S0	1	Intrusione
11	TCP	SMTP	S0	1	Intrusione
12	UDP	SMTP	S0	1	Intrusione
13	UDP	HTTP	S0	0	Intrusione
14	ICMP	SMTP	S1	1	Normale

L'algoritmo del DT trova per primo la caratteristica migliore (quella con information gain più alto) utilizzando le equazioni 3.1, 3.2 e 3.3. La selezione della caratteristica procede in questo modo:
Prima viene calcolato Info(D):

$$\text{Info(D)} = -(9/14) \times \log_2(9/14) - (5/14) \times \log_2(5/14) = 0.940 \qquad (3.4)$$

Dove (9/14) è la probabilità di intrusione mentre (5/14) è la probabilità di attività normale.
Dopodiché viene calcolato il guadagno informativo per ogni caratteristica.

Ad esempio, a seconda del Protocol Type:

$$\text{Info}_{ProtocolType}(\text{D}) = (5/14)\times I(2,3)+(4/14)\times I(4,0)+(5/14)\times I(3,2) = 0.694 \quad (3.5)$$

Dove (5/14)×I(2,3) significa che per il protocollo TCP ci sono 5 istanze su 14 con 2 Intrusioni e 3 pacchetti Normali; (4/14)×I(4,0) significa che per il protocollo UDP ci sono 4 istanze su 14 con 4 Intrusioni e 0 pacchetti Normali e così via per il protocollo ICMP. Infine

Gain(Protocol Type) = Info(D) - $\text{Info}_{ProtocolType}$(D) = 0.246

Allo stesso modo, Gain(Service) = 0.029, Gain(Flag) = 0.151 e Gain(Land) = 0.048. In questo caso Gain(Protocol Type) è più alto delle altre caratteristiche perciò il DT Classifier sceglie per primo Protocol Type. Questa procedura è applicata ricorsivamente per costruire l'albero decisionale T, mostrato in figura 3.3.

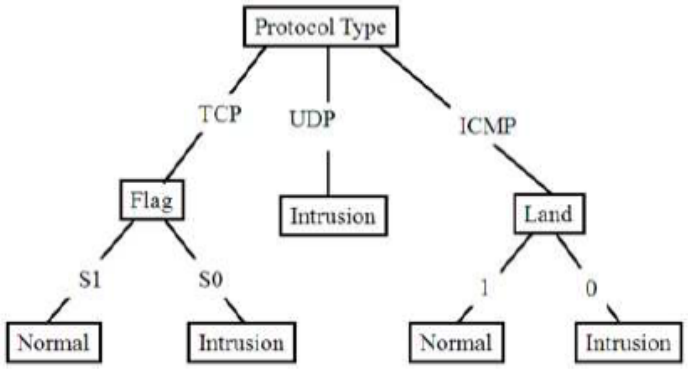


Figura 3.3: Albero decisionale

Dopo aver costruito l'albero decisionale T, vengono generate delle regole per ogni percorso dalla radice a ogni foglia di T.

Avendo un pacchetto sconosciuto X = (Protocol Type = TCP, Service = SMTP, Flag = S0, Land = 0) applicandolo al DT Classifier scopriamo tramite la regola 2 che il pacchetto è una intrusione; in questo modo il DT Classifier stabilisce le classi di pacchetti sconosciuti nel cloud.

Tabella 3.2: Regole derivate

No.	Rule	Risultato
1	If Protocol Type = TCP AND Flag = S1 Then	Normal
2	If Protocol Type = TCP AND Flag = S0 Then	Intrusion
3	If Protocol Type = UDP Then	Intrusion
4	If Protocol Type = ICMP AND Land = 1, Then	Normal
5	If Protocol Type = ICMP AND Land = 0, Then	Intrusion

3.3 Valutazione del NIDS nel cloud

3.3.1 Setup

Per testare il modulo NIDS è stato utilizzato un cloud open source chiamato Eucalyptus installato su sistema operativo Ubuntu. Il modulo NIDS è installato sul back-end; viene utilizzato Scapy per inviare pacchetti personalizzati sulla rete; sia su front-end che su back-end è eseguito Wireshark per monitorare il traffico; per il logging delle intrusioni viene utilizzato un database MySql.
Per il training del DT Classifier sono stati utilizzati due dataset, il NSL-KDD e il KDD. Il KDD è uno dei pochi dataset pubblici per il machine learning mentre il NSL-KDD è un miglioramento del KDD mirato a sopperire ad alcuni difetti nel KDD.
Le class labels dei training set erano 25 ma sono state convertite in solo due: Normal ed Intrusion. Le caratteristiche in questi dataset erano 41 ma ne sono state utilizzate 17 in quanto la classificazione di 41 caratteristiche del dataset KDD diminuisce la precisione di rilevamento. Le caratteristiche con valori continui (src_bytes, dst_bytes, count e srv_count) sono state normalizzate in 100 blocchi di dimensione 500.
E' stata calcolata la percentuale di veri positivi (TPR), falsi positivi (FPR), veri negativi (TNR), falsi negativi (FNR), fitness, F_score, accuracy e costo computazionale per valutare l'adeguatezza del modulo NIDS all'utilizzo nel Cloud.

3.3.2 Risultati e discussione

I risultati sono riportati in tabella 3.3. Viene mostrato che il NIDS ha precisione alta (maggiore di 95%) in entrambi i dataset. La percentuale di veri positivi è più alta nel KDD e mostra che il 96.25% delle intrusioni viene riconosciuto come Intrusione. In entrambi i dataset il TNR è più alto del TPR, ciò significa che il NIDS predilige il non generare allarmi inutili.

Tabella 3.3: Performance results

Dataset	Precision	TPR	TNR	FPR	FNR
NSL-KDD	95.45	76.80	95.15	4.85	23.20
KDD	99.32	96.25	98.08	1.92	3.75

Indicati in tabella 3.4 sono fitness, accuracy e F_score. Il valore di fitness valuta quanto il modulo riesca a rilevare bene le intrusioni in presenza di predizioni sbagliate, mentre l'accuracy indica la percentuale di predizioni veritiere. Lo F_score è la media armonica tra TPR e precision dove la precision indica la percentuale di intrusioni avvenute che sono state rilevate dal NIDS.

Tabella 3.4: Performance results

Dataset	Fitness	Accuracy	F_score
NSL-KDD	72.00	84.31	85.11
KDD	94.33	96.71	97.76

Come mostrato nelle figure 3.4 e 3.5, servono meno di 2 secondi al NIDS per testare le 311,029 istanze di dato del KDD, mostrando un costo computazionale basso. Il sistema è facilmente scalabile in quanto possono essere aggiunte nuove regole a Snort senza modificare quelle preesistenti; inoltre, i moduli NIDS possono essere aggiunti e rimossi dal Node Controller senza modificare quelli esistenti, visto che ogni modulo NIDS agisce indipendentemente. Il NIDS proposto è compatibile con ogni protocollo di comunicazione e piattaforma come Windows e Linux.

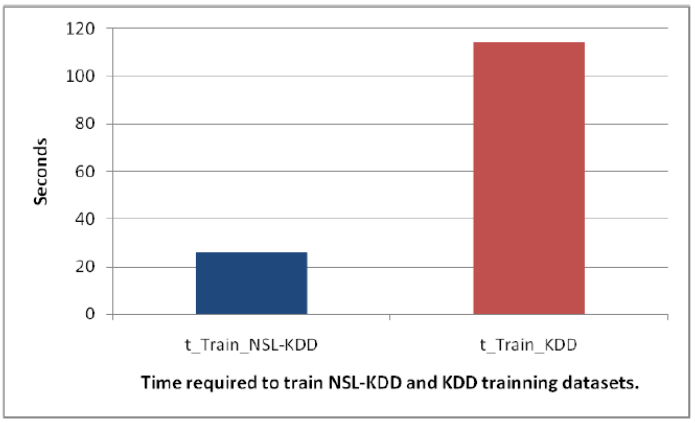


Figura 3.4: Tempo di training necessario al NIDS

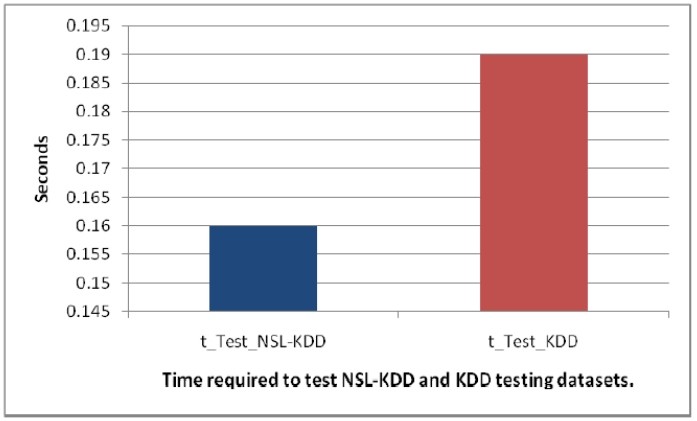


Figura 3.5: Tempo di testing necessario al NIDS

Capitolo 4

Conclusioni

Il cloud computing è in perenne sviluppo; mano a mano che il campo progredisce, emergeranno di sicuro ulteriori vulnerabilità mentre altre diverranno meno rilevanti. Il problema della privacy dei dati diventa più prominente rispetto alle reti tradizionali in quanto il cliente perde il controllo fisico sui dati, e si deve fidare del provider. Le aziende spesso non si fidano a cedere il controllo dei propri dati, evitando quindi di migrare verso una soluzione cloud. Un'altra complicazione è la difficoltà con cui avviene il cambio di provider.

Il grosso problema comune a queste questioni è la mancanza di standard e certificazioni a cui il provider può essere conforme che danno sicurezza al cliente. La presenza di standard in quanto ad API e interfacce di gestione faciliterebbe la migrazione da un provider ad un altro evitando il lock-in, mentre clausole specifiche nei Termini di Utilizzo e nel Service Level Agreement dovrebbero mettere in chiaro aspetti che risultano importanti per quanto riguarda la fiducia trasmessa al cliente. Ad esempio, i cloud provider dovrebbero rilasciare ai clienti i propri rapporti riguardo lo stato della sicurezza dell'infrastruttura e la valutazione dei rischi. La difficoltà dei servizi cloud ad essere conformi a certi tipi di standard li esclude totalmente da certi utilizzi: ad esempio le organizzazioni che gestiscono le informazioni delle carte di credito dei clienti devono per forza essere conformi allo standard PCI DSS (Payment Card Industry Data Security Standard), tuttavia l'implementazione dei controlli requisiti da questo standard in ambiente cloud risulta esageratamente complicata, perciò non ci sono servizi cloud che offrono questa funzionalità.

Non tutti i problemi riguardano il provider ma anche il cliente cloud è responsabile della sicurezza dell'ambiente cloud, criptando i dati memorizzati nel cloud per maggiore sicurezza ed evitando di aggiungere contenuto pericoloso alla sua parte di cloud. Sia i clienti che i provider cloud vanno educati ai rischi e alle buone pratiche di sicurezza per l'utilizzo del cloud. In questo senso la Cloud Security Alliance offre training di diverso livello per sensibilizzare gli utilizzatori del cloud sulla sicurezza del cloud computing, oltre a diverse certificazioni per le aziende.

In conclusione, la direzione giusta per un utilizzo più sicuro del cloud e per trasmettere sicurezza ai potenziali clienti è quella di educare i provider alle buone pratiche per la sicurezza del cloud e all'utilizzo di software sicuro, poi stabilire standard potenti ai quali le aziende provider devono aderire, che comprendono un certo livello di sicurezza interna al cloud e feedback su richiesta verso l'utente, come ad esempio lo stato di sicurezza del cloud e la locazione fisica dei propri dati.

Ringraziamenti

Ringrazio la mia famiglia e miei amici, che mi sono stati vicino e mi hanno dato supporto durante questo percorso di studi.

Bibliografia

[1] Secunia advisories. http://secunia.com/advisories/37081/, http://secunia.com/advisories/36389/.

[2] C. S. Alliance. Top threats to cloud computing v1.0, 2010.

[3] A. Behl. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *World Congress on Information and Communication Technologies (WICT), 2011*, Mumbai, 2011.

[4] E. S. Bernd Grobauer, Tobias Walloschek. Understanding cloud computing vulnerabilities, 2011. www.computer.org/security.

[5] R. Buchanan. Call centres infiltrated by gangs. http://news.bbc.co.uk/2/hi/uk_news/scotland/glasgow_and_west/6089736.stm.

[6] J. S. Cindy Cohn. Megaupload and the government's attack on cloud computing. https://www.eff.org/deeplinks/2012/10/governments-attack-cloud-computing.

[7] G. H. Daniele Catteddu. Cloud computing, benefits, risks and recommendations for information security, 2009.

[8] S. H. Farhan Bashir Shaikh. Security threats in cloud computing. In *6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, 2011.

[9] S. Farzad. Cloud computing security threats and responses. In *International Conference on Communication Software and Networks (ICCSN), 2011 IEEE 3rd*, Xi'an, 2011.

[10] K. Kortchinsky. Secunia advisories. http://www.immunityinc.com/documentation/cloudburst-vista.html.

[11] W. Liu. Research on cloud computing security problem and strategy. In *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference*, Yichang, 2012.

[12] B. Schneier. Homomorphic encryption breakthrough. http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html.

[13] M. R. P. Srinivasanm Sarukesi, Rodrigues. State-of-the-art cloud computing security taxonomies: A classification of security challenges in the present cloud computing environment. In *ICACCI '12*, Chennai, India, 2012.

[14] Wikipedia. Cloud computing. http://en.wikipedia.org/wiki/Cloud_computing.

[15] Wikipedia. Information security. http://en.wikipedia.org/wiki/Information_security.

[16] Wikipedia. Sicurezza informatica. http://it.wikipedia.org/wiki/Sicurezza_informatica.

[17] K. M. Yashpalsinh Jadeja. Cloud computing - concepts, architecture and challenges. In *2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]*, Kumaracoil, 2012.

[18] Yi-Min Wang, Samuel T King et Al. Subvirt: Implementing malware with virtual machines. 2006.