

"MONITORAGGIO ENERGETICO ED AMBIENTALE"

STUDIO DI FATTIBILITA' PIATTAFORMA METERING

Data Manipulation, Modeling e Dashboarding

Codice rapporto:

C3_Data-Manipulation-Modeling-Dashboarding_COTRAL_0

Prepared by:

Federico Grione

Nella tabella che segue sono indicate le revisioni del documento.

Documento: **C3_Data-Manipulation-Modeling-Dashboarding_COTRAL_0**

Date	Version	Provided	Review	Approved	Main Changes
19/07/2022	01	FG	FG	FG	Prima emissione

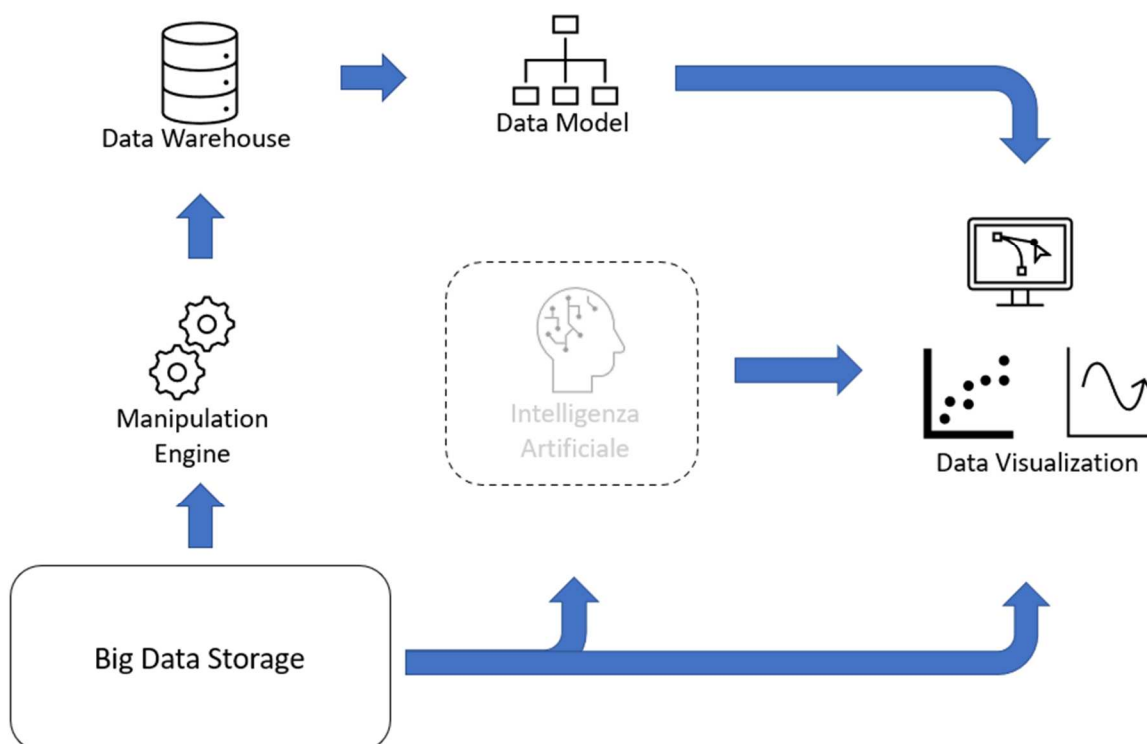
Indice

Indice	3
1 Criteri di valutazione di una soluzione di gestione ed analisi dei dati	4
1.1 (Big) Data Storage / Data Warehouse (DWH).....	4
1.2 Data Manipulation Engine	5
1.3 Data Model	6
1.4 Data Visualization.....	6
2 Criteri di scelta della piattaforma.....	7
3 Cloud vs On Premise	8
3.1 Confronto Cloud Vs On Premise nel contesto generale	8
3.2 Confronto Cloud Vs On Premise nel contesto Data Analytics per IoT	9
3.3 Il Cloud è un ecosistema certificato per diverse Industry, casi d'uso, architetture standardizzate e tecnologie IoT / Energy	10
3.4 Sostenibilità ambientale del Cloud.....	11
3.5 Progettazione architetturale e approccio al Cloud	11
3.6 Resilienza del Cloud computing	12
3.7 Gestione della sicurezza nel Cloud.....	17
4 Servizi IAAS, PAAS, SAAS.....	21
4.1 IAAS (Infrastructure-As-A-Service)	22
4.2 PAAS (Platform-As-A-Service)	22
4.3 SAAS (Software-As-A-Service)	23
5 Schema generale di architettura	24

1 Criteri di valutazione di una soluzione di gestione ed analisi dei dati

I layer in un'architettura di gestione del dato sono principalmente quattro:

- (BIG) DATA STORAGE / DATA WAREHOUSE
- DATA MANIPULATION / PREPARATION ENGINE
- DATA MODEL
- DATA VISUALIZATION



1.1 (Big) Data Storage / Data Warehouse (DWH)

Partendo dal layer di storage è necessario valutare 3 elementi per decidere quali siano le componenti architetturali da prendere in considerazione. Tali elementi sono:

- La quantità di dati da gestire
- La tipologia di dati in gioco
- Le necessità relative all'analisi

La quantità di dati da gestire ha impatto sulle tecnologie di salvataggio e storicizzazione in quanto è preferibile salvare enormi moli di dati in storage a basso costo piuttosto che in un database relazionale. Questo sia per motivi puramente economici che per motivi prettamente tecnici legati al degrado delle performance dei database relazionali oltre un certo limite.

La quantità di dati da gestire impatta anche sulle logiche di storicizzazione delle informazioni poiché mantenere dati grezzi provenienti da sensori IoT o da altre fonti dato richiede una programmazione dello spazio a disposizione sul lungo periodo.

Una volta identificata e definita la quantità di dati che si devono gestire quotidianamente e globalmente, è necessario valutare quali tipologie di dati si dovranno gestire poiché non è sempre possibile salvare informazioni in formato tabellare strutturato, sempre di più le analisi vengono fatte utilizzando dati semi-strutturati (come file json, xml, ecc.) o completamente destrutturati (quali immagini, video, audio, ecc.). La tipologia di dato quindi vincola la scelta della tecnologia di salvataggio delle informazioni e, di conseguenza anche quella di manipolazione.

Relativamente alle necessità di analisi è utile identificare a priori se si desidera analizzare i dati grezzi oppure è sufficiente lavorare su aggregazioni di essi in modo da avere una panoramica sui dati provenienti dalle varie sorgenti.

Tipicamente, quando mole e tipologia di dati lo giustificano, si utilizza uno storage per il salvataggio dei dati grezzi e un database relazionale (nella struttura di un data warehouse) per salvare aggregazioni di dati relazionando le varie informazioni tra loro. Uno Storage per la data analytics è un sistema di salvataggio che consente di gestire i dati come file od oggetti e viene presentata all'utente un'interfaccia di navigazione che ricorda il filesystem di un PC.

Invece, un Data Warehouse (abbreviato in DWH), è una particolare strutturazione di database relazionali tipicamente su 3 livelli all'interno dei quali i dati vengono progressivamente "puliti" e "manipolati/aggregati". Questi 3 livelli storicamente possono prendere diversi nomi, in questo documento li chiameremo Bronze, Silver e Gold.



Il livello Bronze è quello che contiene i dati così come vengono importati dalle sorgenti o dal big data storage (se necessario); il livello Silver è quello dove vengono salvati i dati ripuliti dopo i primi step di Data Quality; Nel livello Gold i dati vengono aggregati e relazionati in modo da poter creare una base per il Data Model.

1.2 Data Manipulation Engine

Il secondo elemento architetturale è il motore dedicato alla lavorazione ed allo spostamento dei dati da una componente all'altra dell'architettura di data analytics.

Come per la componente di salvataggio del dato, anche per quella di lavorazione è necessario capire che genere di elaborazioni devo fare e su quanti e quali dati.

Esistono diverse possibilità di software per fare ETL, dai tool più utilizzati in BI come SQL Server Integration Services (SSIS), Talend, Pentaho e molti altri che forniscono un'interfaccia zero/low-code per movimentare i dati e ripulirli a tool che lasciano maggiore libertà agli sviluppatori ed utilizzano linguaggi come Python, Java, Scala, R ed altri. Il secondo caso è particolarmente utilizzato in ambiti big data.

Nella fase di selezione dell'engine per manipolare i propri dati è fondamentale considerare aspetti come:

- Tipologie di operazioni da effettuare
- Grado di "libertà" per lo sviluppatore
- Competenze tecniche e di sviluppo del team che opera sui dati
- Quantità di dati e necessità di ambienti di calcolo distribuiti

L'obiettivo finale di un motore di elaborazione è quello di preparare delle strutture dati che siano la base dei modelli di analisi. Tenzialmente questa base viene salvata e storicizzata all'interno di Data Warehouse.

1.3 Data Model

I modelli dati sono l'elemento di congiunzione tra la preparazione del dato svolta nel backend e la visualizzazione di dashboard e report. Se nel Data Warehouse confluiscono oggetti che rappresentano le dimensioni di analisi ed i fatti da analizzare salvati in apposite tabelle chiamate appunto "Fatti" e "Dimensioni", il modello dati viene utilizzato per definire al meglio le relazioni tra gli oggetti da analizzare e creare metriche puntuali (o KPI) da monitorare.

1.4 Data Visualization

La data visualization è l'ultimo tassello di un'architettura di data analytics. Si possono utilizzare dei tool specifici di BI che danno la possibilità di costruire con interfacce zero-code i propri report recuperando i dati dalle sorgenti configurate (queste includono DWH, modelli dati, database applicativi, web API, data lake/data storage e molto altro). Esiste anche la possibilità di servirsi di librerie grafiche facilmente reperibili sul mercato che estendono le funzionalità dei più comuni linguaggi di programmazione per dare la possibilità di visualizzare i propri dataset con un grado superiore di configurabilità. Ancora una volta, però, la configurabilità si porta con sé la necessità di competenze specifiche che non sono strettamente necessarie utilizzato tool di BI di mercato quali, tra i più conosciuti: Power BI, Tableau, Qlik e altri.

Questi tool consentono di creare report o dashboard in modo quasi intuitivo costruendo il percorso di analisi sulla base delle proprie esigenze di business. I principali tool di BI consentono di costruire il modello dati all'interno dell'interfaccia di lavoro integrando, di fatto, lo step di creazione del data model all'interno di essi.

La valutazione del tool o della tecnologia da utilizzare per la data visualization dipende da:

- Competenze tecniche di programmazione
- Grado di libertà che si vuole avere nella costruzione dei singoli widget di visualizzazione
- Tempi di sviluppo necessari
- Costi per lo sviluppo e per il licensing
- Performance che si vogliono ottenere in termini di UX ed eventuale refresh dei dati (infatti alcuni tool di BI non sono progettati per gestire grandi moli di dati e refresh in tempo reale)

È altresì possibile integrare dashboard e report sviluppati tramite gli appositi tool di BI all'interno di portali o applicativi web già in essere. Per effettuare questa tipologia di operazione, chiamata embedding, è necessario tenere in considerazione alcuni aspetti legati alla sicurezza ed alla user experience (UX).

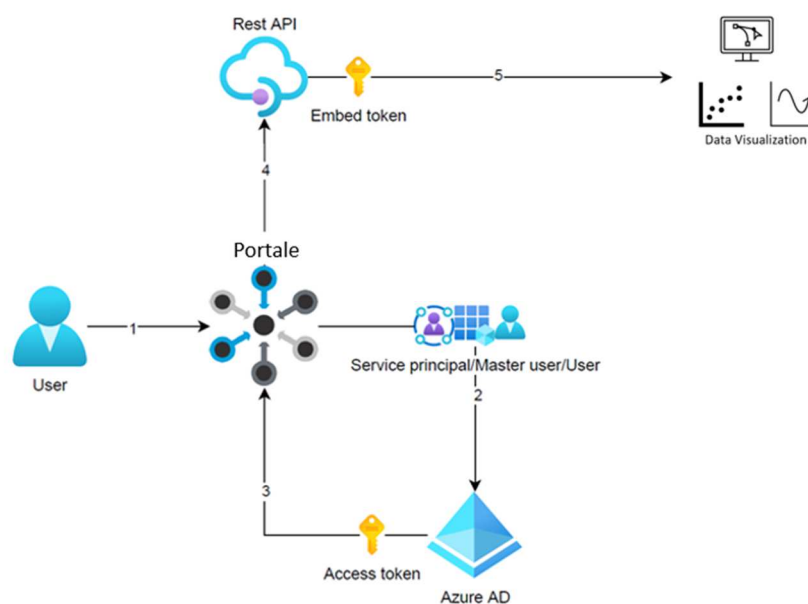
Tali aspetti possono essere riassunti nei seguenti punti:

- incorporare un contenuto già esistente all'interno del portale o applicativo web;

- caricare un contenuto sviluppato tramite il tool di BI non esistente ed incorporarlo all'interno del portale;
- impostare gli aggiornamenti dei contenuti incorporati;
- profilare un utente sulla base della visibilità dei dati (row-level security);
- scaricare in qualche formato consultabile o editabile il contenuto incorporato;
- incorporare contenuti paginati;

Anche gli aspetti di autenticazione sono estremamente importanti. L'embedding deve consentire all'utente di interfacciarsi con sistemi di autenticazioni aziendali utilizzando, per esempio, un token per la sessione in modo da garantire l'autenticazione ai due sistemi (portale/applicativo web e tool di BI).

A titolo di esempio, segue uno schema di embedding utilizzando Azure Active Directory di Microsoft.



Anche la profilazione degli utenti è di fondamentale importanza per garantire l'accesso sicuro alle informazioni, questa si può ottenere grazie a:

- Row-level security: durante la renderizzazione del report viene applicato un filtro ai dati in modo che l'utente abbia accesso solamente alle analisi di propria competenza.
- Report-level security: a livello di portale si può dare la possibilità di profilare un utente in modo che certi contenuti (o report/dashboard) non siano a lui/lei visibili.

2 Criteri di scelta della piattaforma

Una delle scelte cruciali che condiziona un progetto di Data Analytics è dove ospitare i server o i servizi tramite i quali la piattaforma viene eseguita.

Ovviamente per una soluzione IoT di Smart Building e Data Analytics è necessario che i gateway siano ospitati nell'infrastruttura dell'edificio monitorato in modo che possano interfacciarsi con i sensori, soprattutto se essi si attestano sulla rete locale via ethernet o wireless.

Ma la piattaforma deve essere integrata e raggiungibile da tutti gli edifici che, potenzialmente, possono essere distribuiti sul territorio o addirittura nel mondo. Questo aspetto porta spesso ad abbinare la realizzazione di una piattaforma basata su Cloud.

Le principali motivazioni che portano una piattaforma Cloud ad essere adatta ad una soluzione di data analytics su IoT sono le seguenti:

Scalabilità: le necessità delle soluzioni IoT spesso variano nel tempo a causa della crescita del business e, da questo punto di vista, il cloud permette di adattarsi alle diverse esigenze. Grazie al cloud quindi la soluzione permette con relativamente poco sforzo di adattare un'architettura dimensionata per pochi edifici e sensori in un'architettura per centinaia di edifici e sensori.

Sicurezza: il rischio più grande di introdurre delle tecnologie IoT in un processo di business è relativo alla sicurezza. Questo spinge a prediligere soluzioni basate su dei Cloud provider leader nel mercato (Azure, AWS, Google Cloud...) e che facciano largo utilizzo degli strumenti PaaS che vengono messi a disposizione da questi provider, il che assicura l'applicazione di patch di sicurezza e l'utilizzo di crittografia a vari livelli, il tutto senza disservizi.

Gestione & Aggregazione dei Dati: questo aspetto è uno dei più interessanti da valutare perché molto legato alle esigenze del caso specifico. Un aspetto, ad esempio, è legato all'acquisizione in tempo reale che in contesti di monitoraggio remoto è un fondamentale. Nel caso siano necessarie azioni repentine di controllo e attuazione in tempo reale, una strategia utilizzata è l'addestramento di algoritmi AI e ML che possono essere anche eseguiti direttamente nel gateway per eseguire controlli sui dati senza avere ritardi dovuti all'acquisizione.

Usabilità: La piattaforma deve essere facilmente accessibile da chi deve monitorare gli edifici ed essere anche disponibile al responsabile del singolo edificio. Inoltre, deve facilmente permettere l'integrazione con sistemi esistenti. Inoltre, deve presentare e, possibilmente, permettere di configurare delle dashboard.

3 Cloud vs On Premise

3.1 Confronto Cloud Vs On Premise nel contesto generale

La scelta dell'infrastruttura da utilizzare per il progetto è fondamentale al fine del calcolo dei costi complessivi del sistema stesso.

I due principali tipi di architettura sul mercato sono la cosiddetta architettura Cloud (o Cloud pubblico) e on premise (o Cloud privato).

Si può pensare al Cloud come ad una utility company: una soluzione Cloud fa pagare solo quello che si consuma in una formula “a consumo” mentre nella soluzione On Premise tutti gli investimenti iniziali ed i costi sono a carico del cliente finale.

Le principali differenze tra queste due architetture sono le seguenti:

1. Una soluzione On Premise presenta costi di investimenti iniziali più elevati rispetto alla soluzione Cloud in quanto l'infrastruttura fisica deve essere acquistata, installata, configurata e mantenuta dall'utente finale durante tutto il ciclo di vita.

2. La soluzione Cloud presenta costi di gestione inferiori rispetto una soluzione On Premise in quanto non necessita di acquisto iniziale di licenze software e personale adibito al mantenimento dell'hardware e del software.
3. Il Cloud è una soluzione scalabile: in caso di necessità di ulteriori risorse, in una architettura Cloud è sufficiente espandere le risorse in modo semplice e rapido ottimizzando così i costi.
L'operazione di scalabilità può avvenire automaticamente, secondo configurazioni predisposte, oppure mediante riconfigurazione on demand sulla piattaforma del Cloud provider, ed è gestibile sia in modo verticale che orizzontale, ma anche in diminuzione di risorse oltre che di aumento.
La soluzione On Premise invece difetta di questa ottimizzazione e nel caso fosse necessario espandere le risorse in molti casi è necessario acquistare ulteriore equipaggiamento con tutti i costi accessori collegati all'installazione, configurazione e fermo macchina, oltre che le limitazioni legate all'espandibilità e dovute dall'obsolescenza dell'hardware.
4. Una soluzione On Premise necessita di personale interno all'azienda dedicato al mantenimento dell'infrastruttura, la soluzione Cloud è mantenuta dal provider del servizio
5. La soluzione On Premise può presentare nel lungo periodo costi fissi più bassi rispetto alla soluzione Cloud in quanto le macchine vengono ammortizzate così come la manutenzione sempre che non serva espandere le risorse, può inoltre accadere che il costo della sottoscrizione Cloud aumenti nel ciclo di vita del sistema.
6. La soluzione Cloud è maggiormente ottimizzata rispetto ad una soluzione On Premise in quanto nel Cloud solo le risorse effettivamente utilizzate sono allocate, utilizzate e pagate. Nella soluzione On Premise si rischia sempre di avere risorse non allocate o non utilizzate (costi per inutilizzo), così come può succedere anche il contrario ovvero non avere abbastanza risorse disponibili per picchi imprevisti di richieste non soddisfabili a causa della scarsa elasticità / scalabilità dell'infrastruttura stessa.
7. La soluzione Cloud di solito contiene più funzionalità rispetto alla soluzione On Premise: se l'azienda decidesse di costruire e mantenere alcune delle funzionalità On Premise che accompagnano automaticamente la soluzione Cloud, il business case dovrebbe includere anche il costo aggiuntivo di gestione.

3.2 Confronto Cloud Vs On Premise nel contesto Data Analytics per IoT

Nella valutazione tra deployment in cloud oppure On Premise di un'architettura di Data Analytics per IoT, gli elementi principali sono due:

- Sizing dei dati che si dovranno gestire
- Capacità computazionale necessaria

Nell'ipotesi di voler installare l'infrastruttura On Premise, entrambi questi elementi richiedono un'accurata pianificazione del ciclo di vita delle informazioni che verranno gestite dalla piattaforma in modo da poter incamerare e potenzialmente elaborare tutti i dati che, tendenzialmente, saranno in continuo aumento nel corso del tempo.

Si consideri che le piattaforme di Data Analytics, specie se pensate in ottica di applicazione di modelli di machine learning, traggono vantaggio dall'utilizzo di dati storici e quanti più ve ne sono a disposizione, tanto migliori saranno gli output delle analisi e delle previsioni.

L'aspetto del sizing impatta anche sulle capacità computazionali necessarie poiché, maggiore è la quantità di dati da elaborare e maggiore sarà il carico sui motori di elaborazione; è necessario quindi prevedere, oltre al dimensionamento dell'architettura, anche le logiche specifiche di manipolazione dei dati a priori in

quanto, se vi è la necessità di rielaborare frequentemente tutto lo storico dei dati presenti in piattaforma, la capacità computazionale dovrà essere dimensionata di conseguenza.

Viceversa, se sarà sufficiente elaborare periodicamente solo una porzione costante di dati (per esempio relativa sempre e solo all'ultimo mese) e solo saltuariamente vi sarà la necessità di rielaborare una maggior quantità di dati, allora l'aspetto computazionale sarà meno rilevante ai fini della progettazione.

Da un punto di vista pratico, la pianificazione di un'architettura non è banale e la soluzione che semplifica (almeno in parte) questi aspetti è il deployment in cloud in quanto la scalabilità e la flessibilità sono due degli elementi chiave.

Per scalabilità si intende, senza scendere nel dettaglio, la capacità di un'architettura di essere estesa o ridotta; quando la scalabilità viene affiancata alla flessibilità o elasticità, abbiamo una combinazione di fattori che ci permettono di reagire, in termini infrastrutturali, alle reali esigenze del business e di fruizione del dato ottimizzando, di fatto, i costi necessari per implementare un'infrastruttura di Data Analytics.

Altro aspetto da considerare nella valutazione tra cloud e On Premise è la collocazione fisica e geografica dei dati. Sebbene i cloud provider siano molto attenti alle compliance in materia di trattamento dei dati e forniscano documentazione e certificazione su questa, una soluzione On Premise permette di avere il pieno controllo sul proprio patrimonio informativo. Questo aspetto però richiede anche un notevole sforzo per garantire la sicurezza degli accessi e la protezione dei dati stessi in termini di risorse tecnologiche (quindi economiche) ed umane.

3.3 Il Cloud è un ecosistema certificato per diverse Industry, casi d'uso, architetture standardizzate e tecnologie IoT / Energy

Ogni Cloud provider offre una molteplicità di casi d'uso e architetture standardizzate di riferimento, dedicate a diverse Industry tra cui quelle che fanno uso di tecnologie IoT / Energy.

È possibile strutturare la soluzione più adatta alle proprie necessità di business e al caso d'uso specifico, partendo quindi da architetture di riferimento solide in quanto già testate e certificate, alle quali vengono integrati o personalizzati ulteriori elementi / servizi al fine di realizzare soluzioni sofisticate e complesse: l'obiettivo è di concentrare la maggior parte dell'effort proprio sulle peculiarità specifiche del progetto e di minimizzare gli sforzi nella gestione degli elementi standard / di base (quest'ultimo punto è solitamente impattante nel modello On Premise, nel quale vanno implementati e gestiti anche gli elementi costitutivi di base dell'infrastruttura che distraggono in modo importante dal focus del progetto).

A titolo di riferimento:

- Microsoft Azure: soluzioni per l'industria real estate, smart building e facility - <https://docs.microsoft.com/en-us/azure/architecture/industries/facilities-real-estate>
- Amazon AWS: valorizzazione dei sistemi building esistenti con il servizio IoT di AWS - <https://aws.amazon.com/it/blogs/architecture/enhancing-existing-building-systems-with-aws-iot-services/>

3.4 Sostenibilità ambientale del Cloud

Un punto di forza importante del Cloud riguarda la sostenibilità ambientale, tema che in un progetto di Carbon Neutrality è sicuramente da considerare come valore aggiunto, in quanto consente di limitare ulteriormente il carbon footprint che l'organizzazione ha l'obiettivo di ridurre col progetto stesso, evitandone la produzione proprio con le tecnologie che vengono utilizzate per la rilevazione e analisi.

La scelta strategica di adottare il Cloud diventerebbe quindi elemento integrante a supporto dei valori e dell'obiettivo di progetto.

Nel dettaglio, i maggiori Cloud provider sono impegnati attivamente nella riduzione delle emissioni: da almeno un decennio sono già certificati "carbon neutral" (viene rimossa ogni anno una quantità di carbonio pari a quella emessa, mediante compensazione o riduzione) e si sono dati l'obiettivo di diventare "carbon negative" entro il 2030 rimuovendo annualmente più carbonio rispetto a quello emesso. (Addirittura Microsoft su questo ha un obiettivo molto sfidante in quanto entro il 2050 vuole rimuovere tutto il carbonio emesso durante l'attività aziendale, direttamente o tramite consumo di elettricità, fin dalla fondazione nel 1975.)

Oltre alle emissioni, i Cloud provider sono sostenibili dal punto di vista dell'impatto ambientale anche su altre aree: acqua (positività idrica), rifiuti zero, ecosistemi naturali (zero deforestazione da nuove costruzioni).

I risultati delle ricerche evidenziano che il Cloud è tra il 22 e il 93% più efficiente dal punto di vista energetico rispetto ai datacenter aziendali tradizionali On Premise, a seconda del confronto specifico effettuato: tenendo in considerazione gli acquisti di energia rinnovabile dei Cloud provider, questi sono anche tra il 72 e il 98% più efficienti dal punto di vista delle emissioni di carbonio.

Questi risparmi sono attribuibili a quattro caratteristiche chiave del Cloud:

- efficienza operativa dell'IT,
- efficienza delle apparecchiature IT,
- efficienza dell'infrastruttura del data center,
- approvvigionamento di energia elettrica rinnovabile.

In aggiunta a questo, i clienti delle sottoscrizioni dei Cloud provider di primaria importanza hanno a disposizione delle dashboard gratuite che consentono di valutare l'impatto del carbon footprint dei servizi da essi utilizzati, comprendere le emissioni evitate nel tempo grazie all'efficienza dei loro datacenter e stimare ulteriori risparmi energetici.

Fonti di riferimento:

- Microsoft Azure <https://azure.microsoft.com/en-gb/global-infrastructure/sustainability>
- Amazon AWS: <https://sustainability.aboutamazon.com/environment/the-cloud>
- Google GCP: <<https://cloud.google.com/sustainability?hl=en>>

3.5 Progettazione architetturale e approccio al Cloud

Affinché un progetto Cloud-based apporti maggior valore e garantisca il raggiungimento degli obiettivi di

business ed anche di risparmio dal punto di vista economico, è necessario approcciare questo ecosistema secondo la filosofia con cui è stato concepito e seguendo alcune best practice di riferimento:

- il Cloud è un ambiente dinamico ed in continua evoluzione, strutturato per modernizzare ed innovare i processi tecnologici: il continuo aggiornamento dei servizi offerti permette di continuare a migliorare il livello di innovazione e di valore ricavabile dalle informazioni conservate e gestite al suo interno,
- per modernizzare ed innovare è necessario fare le cose in modo nuovo, abbandonando alcuni capisaldi del mondo On Premise ed evitando di trovare la perfetta equivalenza tra oggetti On Premise ed oggetti Cloud, ma studiando la soluzione più adatta per ogni caso.
Ad esempio, cercare di portare una Virtual Machine On Premise così com'è sul Cloud non è un approccio corretto, in quanto prima è necessario valutare globalmente i servizi da essa gestiti, il tipo di carico di lavoro, la disponibilità, la tipologia e quantità di richieste a cui risponde, etc, ed in base a queste informazioni sarà possibile selezionare la soluzione più adeguata che potrebbe spaziare da un serverless computing ad un container in Kubernetes oppure solo in ultima istanza ad una VM se si tratta di uno scenario legacy non modernizzabile.
- l'ampia scelta di piattaforme tecnologiche di diverso tipo (SaaS, PaaS, IaaS) permette di avere a disposizione molte opportunità per risolvere le varie necessità e problemi da affrontare, ed è il giusto mix di queste tecnologie che consente di ottenere il risultato desiderato, considerando anche vincoli come il budget di spesa, il grado di delega della gestione tra provider e utente finale, la profondità di controllo necessario per ogni stack, gli SLA da prevedere.
- l'approccio più corretto, inoltre, è di andare oltre al confronto Cloud Vs OnPremise, adottando un modello Hybrid Cloud che contempli entrambi gli ambienti come un unico ecosistema coeso e integrato, dove l'OnPremise viene considerato come Edge e in quest'area viene elaborata una parte di computing e processamento dei dati prima di inviarli al Cloud, con l'obiettivo di trarre il beneficio massimo da ogni punto.
- nello studio delle architetture, è molto importante l'analisi funzionale al fine di definire i processi ed i flussi tra i vari servizi, e per pianificare in modo ottimale i workload (oggetti e servizi Cloud) con l'obiettivo di ridurre al minimo i costi di computing mediante triggering event based (processi serverless che consumano anche solo pochi secondi di CPU), operazioni batch, variazioni dei profili di servizio nei momenti di inutilizzo per evitare costi inutili, spegnimento e riattivazione programmati di risorse: l'elasticità e la programmabilità del Cloud consentono queste dinamiche di orchestrazione e ulteriori risparmi economici
- un altro aspetto importante che caratterizza i Cloud provider mainstream è il Well-Architected Framework, una serie di principi guida e best practice utilizzabili per migliorare la qualità delle architetture, basati su 5 pilastri fondanti chiamati C.O.R.P.S.:
 - Cost Optimization (Ottimizzazione dei costi)
 - Operations Excellence (Eccellenza operativa)
 - Reliability (Affidabilità)
 - Performance Efficiency (Efficienza delle prestazioni)
 - Security (Sicurezza)

3.6 Resilienza del Cloud computing

La resilienza del Cloud e dei servizi in funzione dello SLA scelto dipende dai seguenti fattori:

- Scalabilità
- Alta Disponibilità (High Availability)
- Alta Affidabilità (High Reliability)
- Protezione dei dati (Data Protection)

Scalabilità

Tutti i servizi (IaaS, PaaS, SaaS) per le varie tecnologie (calcolo, storage, etc) sono disponibili in data center autonomi organizzati per aree geografiche coerenti (Region) che lavorano insieme per garantire la resilienza dei servizi e dei dati e sono scalabili by design.

La scalabilità dei servizi è impostabile in modalità manuale oppure automatica ed è programmabile per gestire picchi periodici: la modalità va valutata in fase di progettazione secondo necessità di progetto e di business ed è variabile nel tempo in seguito a monitoraggi continuativi che mantengono aggiornata la baseline di riferimento.

La piattaforma dovrà essere scalabile rispetto all'aumento dei volumi dati e richieste gestiti.

In questo senso, l'architettura dovrà essere progettata per rispondere a logiche di scalabilità verticale (aumento delle prestazioni di ogni singolo worker) e orizzontale (aumento del numero di servizi worker contemporanei).

Per gestire al meglio i costi, dovranno essere previste logiche di scalabilità in aumento di risorse (scale-up e scale-out) ma anche in diminuzione (scale-down e scale-in), a seconda del flusso di richieste e di baseline di riferimento sull'utilizzo.

Alta Disponibilità (High Availability)

I Cloud sono costituiti da datacenter geograficamente dispersi conformi ai principali standard di settore (come ISO/IEC 27001:2013 e NIST SP 800-53) per la sicurezza e l'affidabilità.

I data center sono gestiti, monitorati e amministrati dal personale operativo del provider, il quale vanta anni di esperienza nell'erogazione dei più grandi servizi online al mondo con continuità 24 ore su 24, 7 giorni su 7.

Ogni Cloud è composto da un'infrastruttura di data center distribuita a livello globale, che supporta migliaia di servizi online e si estende su centinaia di strutture altamente sicure in tutto il mondo, ognuna delle quali è dotata di alimentazione, raffreddamento e infrastruttura di rete affidabili e autonome.

L'infrastruttura è progettata per avvicinare le applicazioni agli utenti di tutto il mondo, preservando la residenza dei dati e offrendo ai clienti opzioni complete di conformità e resilienza.

Ad esempio, Microsoft Azure ha 58 regioni in tutto il mondo ed è disponibile in 140 paesi/regioni.

Una Region è un insieme di data center interconnessi tramite una rete massiccia e resiliente: la rete include la distribuzione dei contenuti, il bilanciamento del carico, la ridondanza e la crittografia del livello di

collegamento dei dati per impostazione predefinita per tutto il traffico all'interno di una Region o in transito tra Region.

I team Infrastructure and Operations dei provider Cloud sono dedicati alla progettazione, costruzione, gestione e miglioramento della sicurezza dell'infrastruttura cloud, garantendo che l'infrastruttura Cloud offra alta disponibilità e affidabilità, alta efficienza e scalabilità intelligente.

Gruppi di continuità e vasti banchi di batterie assicurano la continuità dell'elettricità in caso di interruzione di corrente a breve termine. I generatori di emergenza forniscono energia di riserva per le interruzioni prolungate e la manutenzione programmata. In caso di calamità naturale, il datacenter può utilizzare le riserve di carburante in loco.

Reti in fibra ottica robuste e ad alta velocità collegano i datacenter con altri importanti hub e con gli utenti di Internet. I nodi di calcolo ospitano i carichi di lavoro più vicini agli utenti per ridurre la latenza, garantire la ridondanza geografica e aumentare la resilienza complessiva del servizio. Team di ingegneri lavorano 24 ore su 24 per garantire la disponibilità costante dei servizi.

I Cloud provider garantiscono l'alta disponibilità attraverso il monitoraggio avanzato e la risposta agli incidenti, il supporto ai servizi e la capacità di failover di backup.

I centri operativi distribuiti geograficamente sono operativi 24 ore su 24, 7 giorni su 7, 365 giorni all'anno.

Le reti dei Cloud provider sono tra le più grandi al mondo: la rete in fibra ottica e la rete di distribuzione dei contenuti collegano i data center e i nodi edge per garantire prestazioni e affidabilità elevate.

I Cloud provider conservano i dati in modo duraturo in due luoghi ed è possibile scegliere la posizione del sito di backup: in entrambi i siti, il provider mantiene costantemente repliche multiple dei dati.

Il Cloud è una piattaforma e un'infrastruttura di cloud computing per la creazione, la distribuzione e la gestione di applicazioni e servizi attraverso una rete di data center: in base al numero di risorse specificato dall'utente, vengono create macchine virtuali (VM) in base alla necessità di risorse su hypervisor progettati per l'uso nel Cloud e non accessibile al pubblico.

Il parco macchine dei provider è composto da milioni di server a cui se ne aggiungono migliaia ogni giorno: migliaia di host sono inoltre sottoposti a manutenzione quotidiana attraverso riavvii, aggiornamenti del sistema operativo o riparazioni. Prima che un host possa entrare a far parte del parco macchine e iniziare ad accettare i carichi di lavoro dei clienti, il provider verifica che l'host sia in uno stato sicuro e affidabile. Questa verifica garantisce che non si siano verificate modifiche dolose o involontarie ai componenti della sequenza di avvio durante la catena di fornitura o i flussi di lavoro di manutenzione.

L'architettura di rete Cloud fornisce la connettività da Internet ai data center e qualsiasi carico di lavoro distribuito (IaaS, PaaS e SaaS) sfrutta la rete dei datacenter.

I data center si basano su infrastrutture di rete altamente ridondanti e adeguatamente fornite, distribuite dal provider utilizzando architetture con ridondanza N+1 (necessità più uno) o superiore. Le funzionalità di failover completo all'interno e tra i data center garantiscono la disponibilità di reti e servizi.

La gestione e il funzionamento della rete di produzione dei Cloud è uno sforzo coordinato tra i team operativi che utilizzano diversi strumenti di monitoraggio delle prestazioni dei sistemi e delle applicazioni

nell'ambiente.

Inoltre, utilizzano strumenti appropriati per monitorare i dispositivi di rete, i server, i servizi e i processi applicativi.

Per garantire l'esecuzione sicura dei servizi in esecuzione nell'ambiente Cloud, i team operativi implementano diversi livelli di monitoraggio, registrazione e reporting, facendo uso di metriche con dati storici dettagliati sulla disponibilità dell'intero servizio, non solo dei singoli server.

Alta Affidabilità (High Reliability)

Relativamente all'Alta Affidabilità è necessario considerare scenari di Disaster Recovery e Business Continuity, per proteggere i dati aziendali e la loro disponibilità eseguendo il servizio su più data center geograficamente dispersi con ampie capacità di backup, archiviazione dati e failover.

Le piattaforme che erogano i servizi di cloud computing sono piuttosto flessibili e tengono conto di ogni potenziale disastro.

Il Cloud, soprattutto per quanto riguarda i servizi PaaS, è un ambiente progettato con un approccio di alta affidabilità del sistema e di alta resilienza dei dati in ambienti distribuiti; quindi, anche le soluzioni di alta affidabilità sono strutturate secondo questa filosofia architetturale e seguono le Best Practice definite dal Cloud provider:

- prestazioni e affidabilità dello storage sottostante con criteri di resilienza per proteggere i dati primari (repliche sincrone per la ridondanza locale nel datacenter);
- distribuzione dei servizi in più datacenter distribuiti sul territorio, al fine di diminuire la probabilità di guasti e supportare la ridondanza dei servizi, per garantire la Business Continuity;
- replica dei dati primari in datacenter secondari per avere una seconda copia in un luogo separato da quello primario (ridondanza di zona/regione/geografica) e anche una terza copia per le soluzioni mission-critical, al fine di garantire non solo la Business Continuity ma anche il Disaster Recovery (BCDR);
- il backup per i servizi PaaS è inteso come snapshot o versioning, tecnologie in grado di garantire un ripristino granulare da istanze point-in-time dei dati che si verificano - a seconda del servizio - in modo programmato o automaticamente ogni volta che i dati vengono alterati (modifica, cancellazione, ecc.);
- in un ambiente così dinamico e distribuito, per garantire le modalità di protezione dei dati di cui sopra, i supporti di memorizzazione di queste copie di backup sono basati su disco perché è il tipo di supporto più adatto per prestazioni, disponibilità ed espandibilità dinamica della capacità di memorizzazione.

Anche le architetture software e la logica applicativa in questo contesto devono essere progettate tenendo conto del comportamento dello storage e delle strutture dati sottostanti per garantire in modo completo la Cloud Data Governance.

Protezione dei dati (Data Protection)

L'infrastruttura globale dei Cloud è progettata e realizzata a ogni livello per offrire ai clienti i massimi livelli di ridondanza e resilienza ed è composta da aree geografiche, Region e zone di disponibilità (Availability Zone), che limitano il raggio d'azione di un guasto e quindi il potenziale impatto sulle applicazioni e sui dati dei clienti.

La struttura delle Availability Zone è stata sviluppata per fornire una soluzione software e di rete per la protezione contro i guasti dei data center e per fornire una maggiore alta disponibilità (HA).

Le Availability Zone sono posizioni fisiche uniche all'interno di una Region: ogni zona è costituita da uno o più data center con alimentazione, raffreddamento e rete indipendenti.

La separazione fisica delle zone all'interno di una Region limita l'impatto sulle applicazioni e sui dati dei guasti della zona, come le inondazioni su larga scala o altri eventi che potrebbero interrompere l'accesso al sito e la disponibilità delle risorse.

Le Availability Zone e i datacenter associati sono progettati in modo tale che se una zona è compromessa, i servizi, la capacità e la disponibilità sono supportati dalle altre Availability Zone della Region.

Tutti i servizi di gestione sono progettati per essere resilienti ai guasti a livello di Region. Nello spettro dei guasti, i guasti di una o più Availability Zone all'interno di una Region hanno un raggio di guasto minore rispetto a un guasto dell'intera Region.

I provider possono riprendersi da un guasto a livello di zona dei servizi di gestione all'interno di una Region: a tal proposito viene eseguita la manutenzione critica una zona alla volta all'interno di una Region, per evitare che eventuali guasti abbiano un impatto sulle risorse dei clienti distribuite nelle Availability Zone all'interno di una Region.

Una Availability Zone è un'offerta ad alta disponibilità che protegge le applicazioni e i dati dai guasti del data center.

I servizi ridondanti per zona replicano le applicazioni e i dati tra le Availability Zone per proteggere da singoli punti di guasto.

Nel contesto delle zone vengono intesi i diversi livelli di ridondanza e protezione dei dati mediante repliche che possono interessare:

- Ridondanza a Replica Locale: i dati sono replicati in modo sincrono in tre copie all'interno del datacenter
- Ridondanza a Replica di Zona: i dati sono replicati in modo sincrono in tre copie, ciascuna in datacenter fisicamente separati all'interno dell'Availability Zone
- Ridondanza a Replica Geografica: i dati sono replicati in tre copie in modo sincrono nella Region primaria ed in tre copie in modo asincrono in una Region secondaria geograficamente separata dalla prima

Oltre alla replica è possibile configurare ulteriori processi automatizzati di backup e data protection che vanno a supportare situazioni di cancellazione accidentale, involontaria, corruzione dei dati oppure anche dolosa da parte di soggetti o strumenti malintenzionati, che si possono a loro volta appoggiare agli strumenti di storage con disponibilità elevata su cui poggiano le copie primarie.

3.7 Gestione della sicurezza nel Cloud

Nel Cloud ci sono diversi aspetti di security da considerare:

- Sicurezza fisica
- Crittografia
- Gestione delle chiavi e dei secret
- Identities, autenticazione e autorizzazione
- Network security
- Riservatezza delle informazioni
- Monitoraggio e controllo
- Certificazioni, compliance e trust
- Best practice, security controls e benchmarks

Sicurezza fisica

I Cloud provider progettano, creano e gestiscono i Data Center in modo da controllare rigorosamente l'accesso fisico alle aree in cui vengono archiviati i dati dei clienti e si impegnano a proteggere i Data Center che li contengono.

Ogni provider ha una divisione dedicata alla progettazione, alla realizzazione e alla gestione delle installazioni fisiche che supportano i datacenter: questa si occupa di mantenere una sicurezza fisica all'avanguardia.

Crittografia

Per proteggere i dati nel Cloud e garantire confidenzialità, integrità e disponibilità è necessario avvalersi di tecnologie di crittografia tenendo conto dei possibili stati in cui possono trovarsi i dati e dei controlli disponibili per quello stato.

Le best practice per la sicurezza e la crittografia dei dati in Cloud riguardano i seguenti stati dei dati:

- At rest (a riposo): include tutti gli oggetti di archiviazione delle informazioni, i contenitori ed i tipi che esistono staticamente su supporti fisici, siano essi dischi magnetici o ottici, erogati sotto forma di file, disk, blob, table storage, etc,
- In transit (in transito): quando i dati vengono trasferiti tra componenti, sedi o programmi, sono in transito. Esempi sono il trasferimento in rete, attraverso un service bus (da sede a Cloud e viceversa, comprese le connessioni ibride) o durante un processo di input/output.

Gestione delle chiavi e dei secret

Ciascun provider Cloud offre uno strumento dedicato alla gestione di chiavi di crittografia, secret, stringhe di connessione e certificati, mediante il quale è possibile gestire il ciclo di vita di tali oggetti di security dalla generazione, alla rotazione/disattivazione, al rinnovo, ma anche l'accesso controllato da parte di utenti e servizi Cloud (es. web application) che li devono utilizzare per autenticarsi verso altri servizi (es. database) senza doverli specificare direttamente nel codice o nelle configurazioni, limitando quindi l'esposizione di tali oggetti di security a soggetti non autorizzati.

Identities, autenticazione e autorizzazione

La gestione delle identità digitali è affidata alle soluzioni centralizzate di Directory Services e di Identity and Access Management (IAM) che consentono di archiviare in modo sicuro e centralizzato i security principals (utenti, gruppi, service principals, managed identities, applicazioni) mediante i quali è possibile gestire l'autenticazione da parte di utenti, applicazioni e servizi.

Per quanto riguarda le autorizzazioni di accesso ai servizi, alle risorse ed oggetti Cloud è possibile applicare delle ACL o delle policy che si basano su RBAC (Role Based Access Control) o ABAC (Attribute Based Access Control).

L'accesso ai servizi deve essere gestito secondo il principio del minimo privilegio necessario e utilizzando il protocollo più adatto a seconda del contesto (OAuth, SAML, etc).

Network security

Nonostante il Cloud sia un ambiente notoriamente pubblico e condiviso, è possibile configurare il proprio ambiente e servizi in modo tale da isolarli completamente dalla Internet pubblica, mantenendo un accesso dedicato e privilegiato dalla rete OnPremise del cliente (VPN o collegamenti diretti dedicati/ibridi) ed esponendo su Internet solamente eventuali servizi necessariamente raggiungibili ad un pubblico esteso di fruitori (es.: portali web): questa pratica consente di ridurre considerevolmente la cosiddetta superficie di attacco.

Sul layer di networking privato sono presenti diverse tecnologie per realizzare questo scopo, le cui principali sono:

- **Virtual Network:** una rete virtuale è un costrutto logico costruito sopra il tessuto di rete fisico del provider. Ogni rete virtuale è isolata da tutte le altre reti virtuali; ciò contribuisce a garantire che il traffico di rete nelle vostre implementazioni non sia accessibile ad altri clienti.
- **Network Security Group:** applicati alle Virtual Network come controllo di base dell'accesso a livello di rete (basato sull'indirizzo IP e sui protocolli TCP o UDP), vengono utilizzati dei Network Security Group. Un NSG è un firewall di base, stateful, con filtraggio dei pacchetti, che consente di controllare l'accesso in base a regole a "5-tuple".
Tale firewall impedisce l'accesso alla risorsa finché non vengono specificati i client autorizzati e concede l'accesso in base all'indirizzo IP di origine di ogni richiesta.
Per configurare il firewall, è necessario creare regole che specifichino gli intervalli di indirizzi IP accettabili oppure i "Service Tag" di servizi o categorie di servizi gestiti nel Cloud.

- VPN: connessione sicura della o delle sedi Cotral al Cloud provider, utilizzando il gateway VPN che collega le reti on-premises al provider tramite VPN Site-to-Site in modo simile a come si configura e si connette una filiale remota. La connettività è sicura e utilizza i protocolli standard del settore Internet Protocol Security (IPsec) e Internet Key Exchange (IKE).
- Private Link: fornisce connettività privata da una rete virtuale al servizio Platform As A Service (PaaS), ai servizi di proprietà del cliente o dei partner. Semplifica l'architettura di rete e protegge la connessione tra gli endpoint in Cloud eliminando l'esposizione dei dati alla rete Internet pubblica. Ad esempio, è possibile accedere ad un servizio PaaS di Database o Data Warehouse solamente da connessione privata e non da rete pubblica, ottenendo quindi il livello di protezione tipico di un servizio On Premise.

Per quanto riguarda il layer di networking pubblico, è possibile avvalersi dei seguenti livelli di protezione:

- piattaforma di servizi Cloud: i router di filtraggio a livello perimetrale e di accesso della rete Cloud forniscono un grado di sicurezza ben definito a livello di pacchetto e impediscono i tentativi non autorizzati di connessione. I router assicurano che il contenuto effettivo dei pacchetti includa dati nel formato previsto e sia conforme allo schema di comunicazione client/server previsto. Nel Cloud viene implementata un'architettura a livelli che consiste nella separazione della rete e nei componenti di controllo dell'accesso dei router perimetrali e di distribuzione (protezione anti-spoofing e controllo dell'accesso RBAC).
- protezione DDoS: è possibile attivare la protezione da attacchi di tipo Distributed Denial of Service sugli oggetti esposti pubblicamente, in modo da evitare non solo interruzioni del servizio a discapito degli utenti reali, ma anche dei surplus di costi dovuti al consumo eccessivo di servizi per rispondere a richieste illegittime.

Riservatezza delle informazioni

Per garantire la massima riservatezza dei dati, con alcuni specifici sistemi di gestione dati Cloud è possibile gestire l'autorizzazione in modo granulare con le funzionalità:

- Row Level Security (RLS)
- Dynamic Data Masking (DDM)

Row Level Security (RLS) semplifica la progettazione e la codifica della sicurezza. Consente di applicare restrizioni all'accesso alle righe di dati nell'applicazione. Ad esempio, limitare l'accesso degli utenti alle righe relative al loro reparto o limitare l'accesso dei clienti solo ai dati relativi alla loro azienda. La logica di restrizione dell'accesso si trova nel livello del database, anziché lontano dai dati in un altro livello dell'applicazione. Il sistema di database applica le restrizioni di accesso ogni volta che si tenta di accedere ai dati da qualsiasi livello. Questa logica rende il sistema di sicurezza più affidabile e robusto, riducendo la superficie del sistema di sicurezza.

È possibile utilizzare anche il *Dynamic Data Masking (DDM)* per limitare l'esposizione dei dati sensibili mascherandoli agli utenti non privilegiati. Può essere utilizzato per semplificare notevolmente la progettazione e la codifica della sicurezza nelle applicazioni.

Il mascheramento dinamico dei dati aiuta a prevenire l'accesso non autorizzato ai dati sensibili, consentendo ai clienti di specificare la quantità di dati sensibili da rivelare con un impatto minimo sul livello dell'applicazione. Il DDM può essere configurato su campi designati del database per nascondere i dati sensibili nei risultati delle query. Con DDM i dati del database non vengono modificati. DDM è facile da usare con le applicazioni esistenti, poiché le regole di mascheramento vengono applicate nei risultati delle query. Molte applicazioni possono mascherare i dati sensibili senza modificare le query esistenti.

Monitoraggio e controllo

I Cloud provider sono dotati di pannelli di controllo (es.: Service Health, Planned Maintenance, Health Alerts) che consentono di visualizzare informazioni in tempo reale sulle prestazioni, sugli incidenti e sullo stato di salute di tutti i servizi; è inoltre possibile visualizzare la cronologia degli eventi e per ogni incidente viene emessa una dettagliata Root Cause Analysis (RCA).

Grazie a questi strumenti è possibile ottenere informazioni accurate, tempestive e dettagliate sui dati relativi alle prestazioni del servizio e sulle attività di manutenzione pianificate, dati giornalieri sulla disponibilità del servizio e sulle prestazioni delle transazioni ed una comunicazione proattiva per evitare qualsiasi tipo di ritardo e di non fattibilità del servizio.

Le piattaforme Cloud garantiscono alte prestazioni dei propri servizi ed è possibile visualizzare metriche e grafici in tempo reale attraverso pannelli integrati in ogni servizio/oggetto.

Per un monitoraggio più analitico e storicizzato è possibile utilizzare strumenti avanzati come Cloud Monitor, Log Collector e Analytics; metriche, tracing e log delle applicazioni possono essere analizzati con Application Performance Monitoring (APM) disponibili nelle piattaforme.

Con questi strumenti è quindi possibile gestire e garantire prestazioni elevate delle proprie piattaforme applicative (anche a livello globale) e fornire statistiche storiche dettagliate a supporto delle prestazioni dichiarate, tra cui tempi medi di risposta dei servizi, numero medio di transazioni al giorno, in base all'applicazione e all'ingestion dei dati nel caso di IoT.

Certificazioni, compliance e trust

Ogni organizzazione deve rispettare degli standard legali, normativi o dei framework di sicurezza delle informazioni.

Come organizzazione i Cloud provider sono tenuti a rispettare tali regole globalmente e sono quindi certificati secondo i principali standard internazionali (es.: ISO27001, GDPR, SOC 1-2-3, CIS, CSA STAR, DoD, FIPS, NIST, SOX): a loro volta supportano i propri clienti nell'applicazione degli standard richiesti dal paese in cui quest'ultimi risiedono oppure sono tenuti a rispettare per esigenze di business, garantendo anche la possibilità di definire la residenza dei dati.

Best practice, security controls e benchmarks

A supporto delle attività di gestione della sicurezza i Cloud provider offrono documentazione e strumenti pratici:

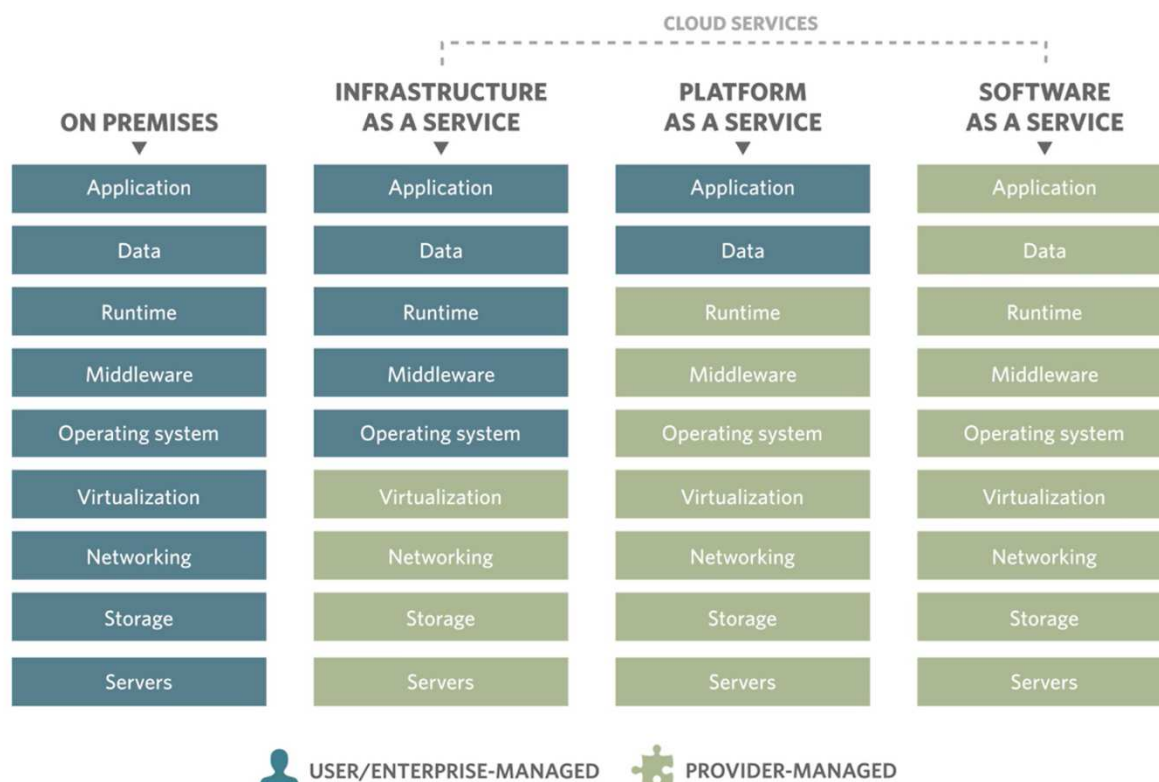
- *Best Practice*: procedure consigliate per la sicurezza da usare durante la progettazione, la distribuzione e la gestione delle soluzioni Cloud, basate sull'esperienza del provider in materia di sicurezza Cloud e dalle esperienze di altri clienti;
- *Security Controls*: raccomandazioni applicabili all'ambiente Cloud che identificano un elenco di stakeholder che sono tipicamente coinvolti nella pianificazione, nell'approvazione o nell'implementazione dei Benchmark;
- *Security Benchmarks*: raccomandazioni che forniscono un punto di partenza per la selezione di specifiche impostazioni di configurazione della sicurezza nell'ambiente e permettono di ridurre rapidamente i rischi per l'organizzazione.

Tali strumenti sono basati su standard di organizzazioni riconosciute a livello internazionale come CIS e CSA e su framework di sicurezza standard come ISO 27001 e NIST.

I Cloud provider, inoltre, rendono disponibili strumenti che supportano le fasi di assessment, verifica, alerting e remediation già integrati nella piattaforma Cloud e utilizzabili per attività continuative, al fine di garantire la sicurezza durante tutto il ciclo di vita dell'ambiente, dalla realizzazione seguendo le continue evoluzioni.

4 Servizi IAAS, PAAS, SAAS

Analizziamo ora le diverse tipologie di servizio considerando ogni livello che le compone e le diverse responsabilità dell'utente finale e del provider per ciascun caso:



4.1 IAAS (Infrastructure-As-A-Service)

Questo servizio si occupa di rendere disponibile infrastruttura on premise quali: macchine virtuali, storage e networking in maniera scalare.

Generalmente si utilizza questo servizio per carichi di lavoro temporanei, sperimentali o che cambiano in maniera inaspettata. Rispetto a soluzioni On Premise utilizzare un servizio IAAS permette di ridurre costi e avere un carico di lavoro sempre ottimizzato in quanto le risorse si possono scalare a seconda delle esigenze.

I principali vantaggi sono elevata flessibilità, facile messa in opera di risorse, cosa che può anche avvenire automaticamente a seconda del carico di lavoro.

L'infrastruttura, infatti, è noleggiata "a consumo" ovvero si paga solo quello che effettivamente si va ad utilizzare, e il cliente finale detiene il completo controllo dell'infrastruttura.

Le tipiche difficoltà che si possono incontrare quando si vuole utilizzare questo tipo di servizio sono:

- necessita di manutenzione, il monitoraggio e management non sono sempre lineari e la disponibilità dell'infrastruttura dipende dal provider del servizio,
- chi acquista una soluzione di tipo IAAS deve effettuare operazioni quale l'installazione del sistema operativo, dei middleware, il sistema di runtime, la gestione dei dati e le applicazioni conseguentemente a ciò è necessario avere persone che si occupino del mantenimento dell'infrastruttura.

Questo servizio Cloud è quello che richiede più intervento da parte dell'utente finale e quindi è il servizio Cloud che presenta i costi (intesi come TCO: Total Cost of Ownership) più elevati.

4.2 PAAS (Platform-As-A-Service)

Questo tipo di servizio riduce il lavoro all'utente finale in quanto va ad automatizzare tutti i processi relativi a sistema operativo, middleware e runtime lasciando così all'utente la sola gestione di dati e applicazione.

Data Manipulation

Lo scopo principale di un servizio PAAS è quindi quello di fornire una piattaforma dove creare applicazioni senza doversi preoccuparsi dell'infrastruttura sottostante.

I principali vantaggi di PAAS sono:

- semplicità di sviluppo delle applicazioni,
- scalabilità delle risorse,
- manutenzione del software semplificata,
- riduzione del codice necessario a scrivere le applicazioni.

Per contro, si devono considerare le seguenti limitazioni e problematiche:

- integrazione tra data center limitata,
- provider lock-in, ovvero si diventa "dipendenti" dal fornitore del servizio in quanto la migrazione tra un Cloud e l'altro non è sempre possibile senza dover effettuare porting,
- per le soluzioni PAAS non è garantita la retro-compatibilità con sistemi legacy e la migrazione o integrazione non è sempre plug and play,
- il framework che il provider fornisce non è garantito che rimanga invariato per tutta la vita del software e ciò fa sì che nel lungo termine si rendano necessari aggiornamenti software.

Un tipico esempio di PAAS è la creazione di applicazioni personalizzate in Cloud utilizzando servizi messi a disposizione quali ad esempio Azure SQL, Azure Logic App, Azure Functions, Azure IoT Hub, AWS IoT Core, AWS Lambda.

4.3 SAAS (Software-As-A-Service)

Questo servizio completa il processo di astrazione togliendo all'utente il compito della gestione di dati e applicazioni lasciando così all'utente solo il compito di gestire la sicurezza dei dati e l'accesso alle applicazioni. Il provider in questo caso si occuperà della gestione di tutto lo stack informatico.

Un tipico esempio di SAAS sono tutti i software che girano nativi in Cloud come, ad esempio, la suite Office 365 e Power BI.

Questo tipo di servizio elimina inoltre la necessità di avere personale IT specializzato in quanto le applicazioni SAAS non vengono scaricate e installate sul dispositivo ma vi si accede tramite rete pubblica (Internet).

Di contro questo servizio presenta alcuni svantaggi da tenere in considerazione:

- limitata interoperabilità tra applicazioni,
- limitazioni da parte del provider del servizio all'accesso dei dati,
- sicurezza del dato ridotta dovuta al fatto che spesso è necessario trasferire più dati tra l'utente e il backend cloud utilizzando la rete pubblica,
- il provider del servizio ha il controllo totale dell'applicazione e l'infrastruttura quindi eventuali downtime o interruzioni del servizio sono fuori dal controllo dell'utente finale.

In tutti questi servizi il provider si occupa anche di fornire: il servizio di fatturazione, monitoraggio, logging, sicurezza integrata, backup e disaster recovery.

5 Schema generale di architettura

Riprendendo ed estendendo quanto spiegato nel paragrafo relativo ai criteri di valutazione di una soluzione di gestione ed analisi dei dati, un'architettura di questo tipo si compone di 5 layer principali:

1. Layer di ingestion
2. Layer di salvataggio dei dati (o storage)
3. Layer di preparazione o manipolazione
4. Layer di modellazione
5. Layer di presentazione

Questa è solo la base necessaria per mettere i dati a disposizione dei fruitori; infatti, chiunque dovrà accedere ai dati potrà farlo tecnicamente da ciascuno dei livelli ove il dato viene salvato (Store, Prep, Model & Serve) con le opportune accortezze legate agli aspetti di sicurezza.

Questo perché potrebbero esserci degli stakeholder interessati al dato grezzo cioè non elaborato dalla piattaforma ma presentato così come è stato letto dalle sorgenti, in questo caso la fonte sarà il layer di salvataggio.

Altri stakeholder potrebbero essere interessati a dati ripuliti e preparati, come ad esempio i data scientist che devono occuparsi di implementare modelli predittivi. In questo caso la sorgente sarà il layer di preparazione.

Un ultimo esempio potrebbe essere quello di stakeholder interessati a fare degli analytics e prendere dati già correlati con magari metriche già calcolate e condivise. In quel caso il layer di interesse è quello di modellazione.

La modularità di un'architettura di Data Analytics è il punto di forza di queste soluzioni poiché le rendono flessibili ed adattabili a qualunque tipo di esigenza in ambito di raccolta ed analisi dei dati.