Videosorveglianza tra EDGE e CLOUD, due paradigmi in contrapposizione?

di Angelo Carpani | libero professionista, laureato in Ingegneria elettronica presso il Politecnico di Milano, iscritto all'Ordine degli Ingegneri della Provincia di Como (n.2368 sez.A) | esperto nella progettazione di impianti di videosorveglianza in ambito comunale

Introduzione

In un articolo precedente ("Videosorveglianza in cloud, un obbligo per le P.A.?" – essecome online 8/2019) avevo messo in evidenza i vantaggi ma, nel contempo, anche le criticità di un sistema di videosorveglianza in cloud.

Le tecnologie cloud dispongono certamente di una potenza di calcolo (computing) e storage virtualmente illimitate, irraggiungibili dalle solite infrastrutture on-premise, mettendo in sicurezza le informazioni più importanti secondo uno schema di salvataggio e ripristino tipico delle infrastrutture di Disaster Recovery e consentendo di delegare aspetti sistemistici e di gestione dei pacchetti applicativi nel caso di utilizzo di componenti "managed" come **PaaS** (**P**latform **a**s **a** **S**ervice) e **SaaS** (**S**oftware **a**s **a** **S**ervice)

Negli impianti di videosorveglianza vengono, però, sempre più adottate telecamere intelligenti e ad alta risoluzione (4K), con registrazione e video analisi a bordo camera, orientando il mercato verso soluzioni edge per lo storage e il computing. L'evoluzione tecnologica e la miniaturizzazione hanno messo a disposizione capacità molto elevate, in termini di potenza di calcolo e di storage, direttamente alla fonte dei dati, cioè sulla telecamera.

Parliamo di telecamere ma il concetto di edge si potrebbe estendere anche agli NVR che vengono spesso installati per garantire la registrazione in loco delle immagini delle telecamere.

Lo scrivente, ad esempio, sta seguendo da anni il progetto del Parco Nazionale dell'Arcipelago Toscano, che si sviluppa su 6 delle 7 isole dell'arcipelago collegate tra

loro da dorsali wireless ridondate in space diversity e frequency, in cui presso ciascuna isola è stato previsto un NVR allo scopo di garantire le registrazioni a livello locale. Lo stesso concetto, ovviamente, si può estendere anche nell'ambito delle città in cui si vogliono tenere sotto controllo siti particolari (es. musei, parcheggi pubblici, ecc.) che contano la presenza di numerose telecamere ad alta risoluzione.

1. Vantaggi e svantaggi del CLOUD

L'ambiente cloud è ideale per quei processi che richiedono di analizzare enormi quantità di dati; quando però questi ultimi provengono da telecamere poste in localizzazioni remote, sono richieste risorse in termini di banda e latenza che, se non adeguate, rischiano di compromettere la

gestione e la manipolazione realtime dei dati provenienti dal campo: la latenza di rete può risultare inaccettabile per monitorare determinati contesti.

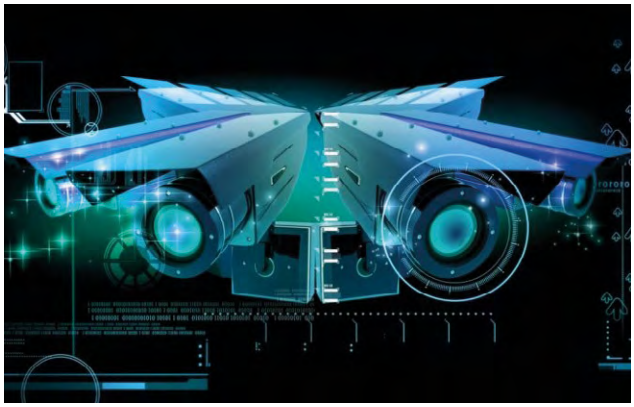
Sebbene l'edge a bordo camera sia lo strumento ideale per la raccolta sul campo di una mole importante di informazioni, questa modalità ha comunque la necessità di un repository intelligente, quindi di una soluzione cloud, per tutti quei dati che devono comunque essere memorizzati, storicizzati e analizzati nel tempo.

Si pensi, ad esempio, agli impianti di videosorveglianza realizzati per finalità di tutela della sicurezza e dell'ordine pubblico in cui le immagini possono essere conservate per un tempo indefinito (diversamente dalle finalità di sicurezza urbana, di competenza delle Polizia Locali o Municipali, in cui le immagini possono essere conservate per un periodo massimo di 7 giorni).

Non è detto, inoltre, che un'architettura distribuita, sia in termini di storage che di computing, sia più semplice o meno complessa di un'architettura cloud centralizzata, dovendo combinare tra loro un'eterogeneità di componenti di rete, anche di produttori diversi, che possono comunicare tra loro attraverso una varietà di interfacce.

Uno dei vantaggi del cloud consiste nella possibilità di esternalizzare alcune infrastrutture, consentendo una riduzione delle spese in "conto capitale" ma aumentando nel contempo le spese, quelle operative e gestionali, in "parte corrente". Ciò consente, appunto, di evitare alcuni investimenti immediati a livello di HW e SW, che andrebbero ammortizzati sul lungo periodo, a favore però di spese correnti da spalmare nel tempo per il pagamento dei servizi esternalizzati. Dalla migrazione dei servizi esterni verso il cloud e la possibilità di pagare soltanto gli effettivi consumi in cui, all'atto pratico, il cliente paga solo ciò che usa (pay-per-use) – con gli unici costi da sostenere che dipendono dallo spazio utilizzato (storage) e dal traffico in uscita (connettività richiesta) - possono derivare risparmi di spesa.

Infine, come accennato nel precedente articolo, nella valutazione del paradigma cloud è importante tenere conto della necessità di prevenire il rischio di lock-in, cioè



la dipendenza esclusiva dal fornitore CSP (Cloud Service Provider) e di un successivo aumento di costi.

2. Vantaggi e svantaggi dell'EDGE

Elaborare e storicizzare i dati all'edge, laddove vengono generati sul campo dalla telecamera, offre numerosi vantaggi in termini di larghezza di banda e di latenza, in particolare quando l'elaborazione in tempo reale sia strategica. É evidente il beneficio in termini di velocità e tempi, con l'eliminazione del trasferimento verso il cloud. Sarebbe interessante sviluppare nella videosorveglianza, anche se nei sistemi di lettura targhe ciò in parte già avviene, una strategia in cui anteporre una raccolta ed elaborazione dati di tipo edge e, solo successivamente, trasferirli in cloud per ulteriori step elaborativi. In termini tecnici: provvedere prima alla creazione di "data lake[1]" sul quale fare successivamente il "data mining[2]". Le soluzioni edge assicurano, inoltre, "resilienza" agli impianti di videosorveglianza in quanto le telecamere possono operare anche in caso di mancanza di connettività garantendo la registrazione delle immagini e la loro video analisi (utile per la registrazione su motion).

Le soluzioni edge, richiedono però una garanzia della sicurezza "fisica": la telecamera deve essere protetta anche nella sua collocazione fisica per limitarne l'accesso al solo personale autorizzato. É evidente che il furto di una telecamera o l'accesso ad una porta della stessa (attraverso uno switch non adeguatamente protetto), con storage a bordo della stessa, mette a disposizione dei

[1]Dall'inglese "lago di dati": un insieme di dati "grezzi" il cui scopo non è ancora definito.

[2]Dall'inglese "estrazione di dati": consiste nell'estrazione di informazioni, precedentemente sconosciute e potenzialmente utili dai dati, al fine di scoprire *pattern* significativi, cioè "modelli" in cui i dati "estratti" siano correlati, abbiano una relazione e siano prevedibili.

malintenzionati tutta una serie di informazioni sensibili. È vero che, come richiede il Garante della Privacy e alcune circolari Ministeriali **(Direttiva del Ministero dell'Interno n.558/SICPART/421.2/70** sui sistemi di videosorveglianza in ambito comunale), la registrazione delle immagini deve avvenire preferibilmente in forma cifrata per garantirne la riservatezza e l'integrità, e l'esportabilità (da locale o remoto) dei filmati deve avvenire con corredo di specifico visualizzatore per la decifratura e verifica dell'integrità degli stessi, ma poi c'è la norma **CEI EN 62676-4** in cui, nella parte dedicata alla memorizzazione ed esportazione dell'immagine, ci dice che "le immagini non devono essere criptate" in quanto "la cifratura può ritardare o impedire il legittimo accesso alle prove video", motivandola sulla base del fatto che comunque "la Polizia assicura che i dati video siano validi per l'uso nell'ambito del Sistema Giudiziario, mantenendo una chiara catena di prova"!
È evidente che, quando implementato in uno scenario corretto, l'edge porta benefici in termini di riduzione del traffico di rete verso il core della piattaforma e riduce i tempi di risposta e latenza degli alert in quanto una parte del workload viene elaborata in periferia. L'edge computing porta intelligenza, capacità di analisi e conseguente possibilità di azione, al di fuori dei datacenter.

3. EDGE e CLOUD, due paradigmi in contrapposizione?

Edge e cloud non sono due paradigmi in contrapposizione, ma devono essere visti come realtà complementari che si integrano fra loro con vantaggi, funzioni e caratteristiche differenti. L'edge deve essere visto addirittura come funzionale al cloud, dato che tra le sue funzioni non c'è solo quello di raccogliere i dati, ma anche quella di filtrarli e aggregarli, permettendo così di ridurre i costi di gestione su cloud, trasferendone successivamente una parte al sistema cloud attraverso specifici protocolli di sicurezza.
Nei moderni sistemi di videosorveglianza, edge e cloud rappresentano quindi due paradigmi che possono coesistere secondo un equilibrio che andrà valutato caso per caso attraverso una BIA (Business Impact Analysis) approfondita, condotta coinvolgendo specialisti IT infrastrutturali ed esperti di cybersecurity oltre che, ovviamente, figure proprietarie di quei dati.
Se il cloud gestisce una enorme quantità di dati che, per la maggior parte, non richiedono risposte in tempo reale, la funzionalità di edge a livello di telecamere favorisce il processo decisionale (es. attivazione di alert) in tempo reale. Edge e cloud possono dunque essere le facce di una stessa medaglia attraverso una ripartizione oculata del carico di lavoro tra telecamere, NVR, sistemi on-premise o cloud.

4. Conclusioni

Nell'articolo precedente (dicembre 2019) avevo accennato anche al cosiddetto principio del **"cloud first"** attraverso il quale le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e/o di sviluppo di nuovi servizi, in via prioritaria devono valutare l'adozione del **paradigma cloud** prima di qualsiasi altra tecnologia e solo qualora il cloud first non soddisfi determinati criteri, si possono sempre utilizzare i sistemi tradizionali che però debbono essere adeguatamente giustificati e la mancata giustificazione può essere addirittura elemento di responsabilità contabile!

É difficile operare in un contesto in cui:

- da un lato (quello della privacy) si raccomanda la registrazione delle immagini in forma criptata e dall'altro (quello normativo) si dice l'esatto contrario;
- in via prioritaria si chiede di valutare l'adozione del paradigma cloud, senza tenere in debito conto l'evoluzione tecnologica dei sistemi di videosorveglianza che evolve sempre più verso l'edge.

Occorre che le diverse agenzie che si occupano di privacy, norme e agenda digitale, dialoghino e si confrontino di più tra di loro, senza imporre rigide regole ad un settore in cui la tecnologia, fortunatamente, evolve rapidamente!