Protezione del dato? La nuova sfida si chiama “Fully Homomorphic Encryption”



Nel mondo d’oggi il dato digitale è oramai un patrimonio prezioso da preservare e difendere più che mai, visti i forti mutamenti in atto in cui vengono abbattuti confini e barriere protettive per consentire una maggior fruibilità delle informazioni ovunque ci si trovi e mediante qualsiasi strumento. Questo ha portato a riconsiderare il forte connubio tra dato ed identità che necessita di una tecnologia capace di protezione indipendentemente dal contesto in cui si opera.

Non passa giorno in cui non leggiamo o addirittura non siamo artefici di una continua crescita di dati generati da processi ed elaborazioni di diversa natura per poi essere trasmessi in rete sia per scopi professionali, governativi o politici, ma anche solo per piacere ed interesse personale.

Se poi pensiamo all’interesse spasmodico ed alla crescita significativa dell’utilizzo del Cloud, così come le nuove tecnologie tipo 5G, l’impiego di sistemi IoT (Internet of Things) fino ad arrivare ai processi di Intelligenza Artificiale (AI), allora possiamo comprendere come tutti questi dati generati e trasmessi tra sistemi eterogenei richieda oramai un approccio alla protezione delle informazioni non più legato al perimetro d’azione in cui si opera, ma ad un nuovo legame intrinseco tra il dato e l’identità che ne deve usufruire.

La crescita del lavoro a distanza, fortemente condizionato dalla pandemia, e l’incremento esponenziale delle transazioni digitali hanno evidenziato come ci sia una forte criticità di esposizione dei dati determinato soprattutto dell’aumento

delle dimensioni della superficie d’attacco che non dobbiamo sottovalutare.

Anzi, in questo contesto notiamo come i team di sicurezza IT si trovino sempre a lavorare rincorrendo le problematiche annesse agli eventi. Questo perché mentre cercano di individuare e fermare gli attacchi devono al contempo trovare un giusto compromesso tra la sicurezza e l’ordinarietà produttiva che costituisce il motore di business per le aziende. Molto spesso si tratta di un equilibrio difficile da raggiungere soprattutto in contesti dinamici ed interconnessi, ed è per questo che assistiamo ad una spinta universale nella ricerca e nello sviluppo di soluzioni e tecnologie mirate ad ottenere una sicurezza sempre più solida e sofisticata.

Seguendo questo approccio, ecco che la crittografia rialza la testa per conquistare un ruolo primario nello scenario mondiale dell’IT proprio come strumento tecnologico avanzato in grado di garantire riservatezza, integrità e disponibilità del dato indipendentemente dall’ambito in cui ci si trovi o dal dispositivo utilizzato per interagire con esso. I sistemi di crittografia avanzati come la “Quantum Key Distribution” e “Homomorphic Encryption” agiscono proprio come tecnologie abilitanti per qualsiasi ecosistema di sicurezza informatica aziendale, fornendo un grandissimo aiuto nel mitigare tutti i problemi e rischi di sicurezza che continuano a sorgere ogni giorno.

Ma andiamo per ordine, partendo dal significato di crittografia.

La crittografia (encryption) viene spesso identificata come quel processo di codifica delle informazioni capace di effettuare una loro trasformazione da un formato in chiaro in un formato cifrato. In realtà conosciamo la crittografia fin dalle sue origini, quando veniva applicata nell’intelligence e nelle operazioni militari. Poi, nel corso degli anni ha subito un’evoluzione davvero significativa tanto da ricevere una

crescente attenzione proprio per la sua capacità di proteggere i dati, sia quando essi si trovano in uno stato “fermo” e cioè memorizzati su dispositivi di storage, sia quando questi sono in “volo” perché trasmessi sulla rete (intranet/internet).

Non solo: la crittografia consente anche di proteggere e rendere più sicuri i dispositivi terminali di front-end con cui quotidianamente interagiamo per manipolare i nostri dati molte volte utilizzando metodi di autenticazione anch’essi cifrati.

Nello specifico possiamo trovare la crittografia applicata in un vasto insieme di situazioni correlate tra loro:

- message encryption
- data loss prevention
- multi-factor authentication
- database encryption
- network encryption
- endpoint devices encryption

In tutti questi casi, la cifratura dei dati si basa sull’utilizzo di “chiavi crittografiche”, siano esse simmetriche o a doppia chiave (pubblica/privata). Le chiavi permettono di crittografare dati leggibili trasformandoli secondo un apposito algoritmo in dati illeggibili. Per poterli decifrare rendendoli nuovamente leggibili, risulta necessario possedere la chiave che ne consenta la loro decifratura.

Con l’evoluzione dei sistemi e delle nuove tecnologie come il Quantum Computing si cominciano ad intravedere situazioni in cui gli attuali protocolli di crittografia e autenticazione potrebbero non essere più sufficientemente sicuri. Ecco perchè si continua a guardare al futuro, molto prossimo, prevedendo un ulteriore step evolutivo riguardo ai metodi avanzati di crittografia, già ora in fase di sviluppo, e che mirano ad affrontare le sfide precedentemente citate. Uno dei metodi di crittografia più innovativo e promettente, soprattutto per gli

ambienti cloud ma applicabile in qualsiasi altro contesto, è costituito dalla Homomorphic Encryption.

Esistono tre tipologie di Homomorphic Encryption: parziale, media e completa.

- PHE (Partially Homomorphic Encryption): protegge i dati ma limitatamente ai due calcoli che possono essere eseguiti su di loro, come l'addizione o la moltiplicazione.
- SHE (Somewhat Homomorphic Encryption): con questa tipologia possiamo eseguire operazioni limitate che possono essere eseguite solo un determinato numero di volte.
- FHE (Fully Homomorphic Encryption): consente ogni tipologia di calcolo ed analisi dei dati mentre sono crittografati, preservando quindi la loro integrità e privacy.

Secondo i massimi esperti quest'ultima risulterebbe una vera e propria novità nello scenario della crittografia mondiale in quanto è in grado di resistere anche ad attacchi di tipo quantistico (Quantum-Safe). Per raggiungere questo grado di sicurezza, FHE richiede una grande potenza di calcolo per l'analisi e presenta ancora qualche limitazione nel supporto multi-utente che lavora con la stessa applicazione sullo stesso gruppo di dati.

Quindi possiamo dire che non è propriamente indicata per l'uso con hardware tradizionale e magari anche datato, ma occorre sicuramente un rinnovo tecnologico che permetta di intraprendere un percorso di protezione del dato con FHE già in fase di ingegnerizzazione delle applicazioni.

Tuttavia, ricerca e sviluppo sono particolarmente attivi nel cercare di perfezionare questa tecnica crittografica, visti i cospicui investimenti degli ultimi anni (si parla di oltre 100 milioni di dollari annui di investimenti globali da parte dei

big del settore come Google, Microsoft e IBM)

Oggi il mercato della crittografia mostra l'esistenza di tecnologie diversificate a seconda del livello a cui si vuole implementare la crittografia, e cioè se allo stato fermo, detto "at-rest" (disco, file system, database), oppure allo stato in movimento, detto "in fly" quando il dato viaggia sulle reti, fino ad arrivare al dato in cloud. Ed è proprio quest'ultima a prendersi la scena in quanto è diventata l'area più rilevante per la maggior parte di aziende ed istituzioni che si apprestano ad utilizzare i servizi in cloud, quindi impegnate a soddisfare determinati requisiti relativi alla protezione ed accesso del dato, cercando di spazzar via tutta quella diffidenza in termini di sicurezza che ancora avvolge gli ambienti cloud.

Certo, per qualsiasi modello cloud (PaaS,IaaS,SaaS) che si sceglie, occorre sempre verificare la compatibilità e la disponibilità di soluzioni di crittografia da parte del fornitore di servizi cloud stabilendo aspettative, capacità e responsabilità dell'intero servizio offerto. Questo è un tema fondamentale per chi si affida ad una infrastruttura in cloud, proprio per evitare debolezze e vulnerabilità non ben considerate e che sono l'origine di tutti gli attacchi a cui assistiamo negli ultimi tempi. Attacchi spesso più pericolosi delle tradizionali campagne di phishing o di virus scaricati navigando in rete, in quanto l'attacco si basa sull'anello debole della catena, individuato spesso nell'uomo, per poi veicolare del codice malevole all'interno dei sistemi. Pertanto gli hacker attendono il momento giusto per completare la loro azione d'attacco e cioè quando la situazione rende il dato più esposto e più vulnerabile.

Ed è questo il punto che mina seriamente la credibilità degli attuali metodi di crittografia per la protezione del dato, creando preoccupazioni relative alla capacità di resistere alle future tipologie di attacco possibili con nuovi mezzi e con tecnologie più potenti capaci di aggredire il dato nel

momento della sua scopertura, cioè quando viene decifrato, ed ecco perché si parla tanto di crittografia omomorfica.

La crittografia FHE mette al sicuro da questo pericolo in quanto il dato potrà essere manipolato ed elaborato da enti terzi senza necessariamente dover essere decifrato. Solo chi detiene la chiave, cioè il proprietario del dato, avrà la capacità di rilevare il suo vero contenuto.

Attenzione però a non soffermarsi esclusivamente sull'algoritmo di crittografia da utilizzare poiché occorre considerare anche la tematica relativa alla gestione delle chiavi di crittografia, che risulta davvero critica.

Oggi, la maggior parte della crittografia utilizza algoritmi a chiave asimmetrica (anche FHE ricade in questa categoria) dove le chiavi utilizzate per la cifrare/decifrare sono diverse. Ciò significa che richiedono sia una chiave pubblica che una privata per accedere ai dati. Di conseguenza, la perdita delle chiavi provoca inevitabilmente la perdita di dati. Ed è proprio questo il tasto delicato che richiede la giusta attenzione, con valutazione di metodologie, processi e soluzioni efficienti e capaci a gestire in totale sicurezza l'intero ciclo di vita delle chiavi

Dando quindi uno sguardo al futuro prossimo, sarà fondamentale per le organizzazioni e per tutti noi comprendere e valutare la pericolosità delle vulnerabilità presenti nel mondo digitale in modo da attivarci per intraprendere una scelta tecnologica in grado di tutelarci e mettere i nostri dati al riparo da ogni pericolo di attacco. Ecco perchè la crittografia avanzata diventerà ben presto un tema centrale per qualsiasi infrastruttura digitale presente e futura

Articolo a cura di **Luigi Perrone**

https://www.ictsecuritymagazine.com/articoli/protezione-del-dato-la-nuova-sfida-si-chiama-fully-homomorphic-encryption/