Attività n. 3.3 - Gestione della sicurezza e tutela dei dati provenienti da un Parco Archeologico

Obiettivi e attività previste

- **Progettazione e Realizzazione di Framework tecnologici e metodologici per la sicurezza dei dati provenienti da un Parco Archeologico**
- **Applicazione delle metodologie proposte alla piattaforma CHIS**

L'evoluzione industriale sta portando a processi di digitalizzazione e all'introduzione di nuove tecnologie, rivoluzionando l'accesso ai flussi di informazioni e incrementando così l'esposizione delle infrastrutture a terze parti. Internet of Things, Cloud Computing, Software Defined Networking e Smart Technologies consentono un livello di connettività tra persone, informazioni, sistemi e risorse mai visto prima, ma allo stesso tempo pongono le moderne organizzazioni di fronte a nuove sfide aziendali. Questi nuovi scenari aprono a nuove significative problematiche nel campo della sicurezza in rete.
Eppure il rapporto tra Internet of Things e sicurezza è ancora conflittuale. Aggiungendo più dispositivi, sensori e oggetti ad una rete si finisce con l'allargare significativamente la "superficie" attaccabile: è necessario, quindi, selezionare con attenzione dispositivi che possano essere configurati e adattati coerentemente con le policy di sicurezza. Si è abbastanza concordi nell'identificare tre principali sfide in termini di sicurezza che l'IoT porta con sé:

Mancanza di standard di sicurezza: una delle sfide più puramente tecniche quando si parla di Internet of Things e sicurezza è la crittografia per i dispositivi più piccoli, come per esempio i sensori. Questi devono infatti funzionare per molto tempo consumando quanto meno possibile. Ciò significa che servono algoritmi e approcci completamente nuovi che possano essere adattati a situazioni simili. Una possibile soluzione è quella della crittografia (LWC). I dispositivi che utilizzano la LWC richiederanno sempre un design specifico, ma l'obiettivo è di standardizzare il livello di sicurezza di questi "mattoni" indispensabili per l'IoT. Uno degli obiettivi del progetto è, quindi, sperimentare queste tipologie di tecniche, e gli approcci su di esse sviluppate, nel contesto di un parco archeologico. Altrettanto interessante sarà sperimentare come tali approcci possano integrarsi con quelli comunemente utilizzati per la protezione di una base di conoscenza come quella costruita nell'ambito del progetto CHIS.

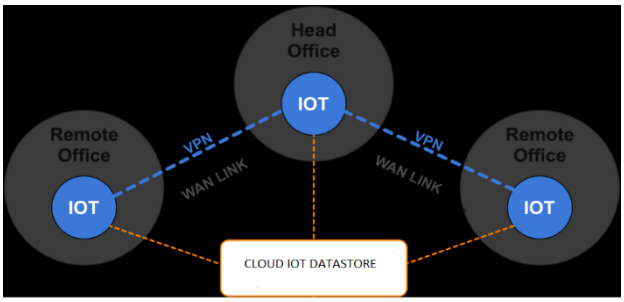
Ulteriore problematica è quella legata ai protocolli di comunicazione diversi che vengono adottati nella comunicazione fra le varie reti di sensori. Alcuni di questi protocolli possono funzionare on top dei protocolli di sicurezza esistenti come per esempio il Transport Layer Security (TLS), che

ha sostituito l'SSL. Questa è una soluzione ideale per i gateway che già supportano il TLS. I dispositivi più piccoli che utilizzano LWC con protocolli di sicurezza basati su messaggi, perché non sono abbastanza potenti per supportare TLS/DTLS, rappresentano invece una sfida più importante. I gateway infatti sono essenziali per la sicurezza dell''IoT perché permettono al traffico di essere ispezionato e convalidato in modo scalabile. Anche in questo caso sarà necessario investigare sul campo le possibili tecniche di risoluzione di questi problemi e sperimentare sul campo approcci e metodologie. Ennesimo problema è quello legato all'aggiornamento dei dispositivi multifunzioni. I dispositivi più piccoli come i sensori non sono aggiornabili. I dispositivi più potenti a funzione singola possono essere aggiornati solo dal loro vendor. Ma i dispositivi multi funzione possono avere software che provengono da vendor diversi e quindi serve un modo affidabile per aggiornare il software senza che questo fatto rappresenti un problema. Gli smartphone hanno già superato con successo questa sfida e il loro approccio viene ora riproposto come Open Trust Protocol (OTrP) dentro lo IETF. Più in generale un grande lavoro per migliorare il rapporto tra Internet of Things e sicurezza si sta facendo con la Online Trust Alliance (OTA), la Cloud Security Alliance (CSA) e il Trusted Computing Group (TCG) per offrire dettagliate linee guida per gli sviluppatori di dispositivi IoT. L'adozione di VPN sia nel caso di sensori IoT che utilizzano SIM (VPN over APN), sia in sensori che utilizzino la connessione radio/internet è sicuramente auspicabile per garantire la sicurezza nella trasmissione di dati. Nell'ambito delle attività di progetto ci si propone di utilizzare questi approcci sperimentandone l'efficacia sul campo.

Nell'ambito dell'attività, inoltre, si provvederà a mettere in sicurezza l'accesso alla base di conoscenza e i dati in essa contenuti. I database nosql investigati saranno *Hadoop*, *MongoDB* e *Cassadra*. La ricerca di alternative ai database relazionali può essere spiegata da due principali esigenze:

- la continua crescita del volume di dati da memorizzare
- la necessità di elaborare grandi quantità di dati in poco tempo.

La scalabilità e la ricerca immediata in quelli che possono essere definiti "document DB" sono le principali caratteristiche che ne giustificano l'uso. Particolare risalto sarà data alla messa in sicurezza dei Big Data: Il punto di partenza che si adotterà per affrontarne la sperimentazione sarà simile a quello utilizzato nella creazione di una strategia di protezione dei dati: determinare i livelli di riservatezza dei dati, identificare e classificare quelli più sensibili, decidere dove collocare le informazioni critiche e stabilire modelli di accesso sicuro a dati e analisi, utilizzando la crittografia ed i meccanismi di sicurezza offerti dai database nosql scelti.



Risultati e deliverables attesi

Risultati attesi

Progettazione ed implementazione di una metodologia per la messa in sicurezza di dati provenienti da una rete di sensori che lavora in accordo ad un paradigma di tipo IoT e di basi di conoscenza di tipo Big Data. Le attività di tipo RI e SS riguarderanno:

- Stato dell'arte e definizione del contesto tecnologico di riferimento (RI).
- Analisi dei principali protocolli ed approcci da utilizzare nell'ambito del contesto di riferimento (RI).
- modellazione e progettazione di un framework per la messa in sicurezza della comunicazione fra i sensori e i Server (SP)
- modellazione e progettazione di un approccio per la messa in sicurezza della base di conoscenza (SP).
- Installazione e test (SP).
- valutazione e validazione del prototipo (RI).

Deliverables

- **DL 3.3.1** Progettazione e realizzazione di un sistema per la messa in sicurezza delle informazioni, organizzato in un base di conoscenza di tipo Big Data come quella definita in CHIS, in un ambiente caratterizzato da un approccio IoT.

Competenze e strumentazioni a disposizione:

Energent S.p.a. possiede al suo interno un'area specializzata nella gestione Big-Data, Cloud e soprattutto sicurezza. Energent S.p.a. ha sviluppato una metodologia di gestione del rischio informatico e trattamento con valutazione positiva Gartner in ambito Europeo (unica azienda Italiana). A tal proposito Energent ha un team di ricerca e sviluppo per la gestione e il trattamento del rischio (sia informatico, sia di accesso ai dati, sia reputazionale, sia perimetrale)

con metodologie e calcolo di formule di rischio ottenute da studi e prototipi sviluppati direttamente da personale interno.
Energent vanta esperienza pluriennale nella gestione di Flussi dati, aggregazione e normalizzazione degli stessi e relativa rappresentazione sia in modalità Grafica che in modalità Geolocalizzazione. La rappresentazione su mappa è a portafoglio Energent sia per le competenze su GIS che per l'utilizzo di open-source la cui configurazione ha permesso di rappresentare le informazioni (di tipo consuntivo e statistico) su mappa Italia con drill-down su regioni, città, cap e singola posizione (longitudine/latitudine).
L'uso di grandi quantità di dati e relativa rappresentazione è stato possibile grazie a contratti con aziende private in ambito Telco ed Energia che hanno messo a disposizioni dati provenienti da sonde fisiche che sono state poi elaborate ed integrate con informazioni acquisite su Open-Data da soluzioni software a portfoglio di
Italdata S.p.A. specializzata nel settore dell'Information & Communication Technology e, in particolare, nello sviluppo di servizi e soluzioni nelle aree dell'e-Government e dell'E-Learning. Uno dei campi di intervento di Italdata è quello delle Smart Cities su cui interviene, tra gli altri, anche nella componente Sicurezza.

Il CONSORZIO STABILE RESEARCH presenta competenze specializzate nel settore della ricerca archeologica e del restauro e valorizzazione del Patrimonio Culturale. Il Consorzio è il promotore di progetti ed iniziative di Ricerca e Sviluppo in collaborazione con Istituzioni Pubbliche e Private e ha svolto una intensa azione di internazionalizzazione.
Il Consorzio attraverso i suoi soci (Research, Arca, Impresa Cosenza, ES) è attivo nel settore delle nuove tecnologie per la documentazione, la tutela, la valorizzazione, la gestione, la sicurezza del Patrimonio Culturale con un focus sulle tecnologie GIS (Geographic Information System) sugli aspetti tecnologico-impiantistici, le applicazioni sul Risk Management, sulla Manutenzione Programmata e sul Monitoraggio.

L'Università di Salerno, nel corso dei progetti CHIS e SNECS, ha sviluppato linee di intervento specifiche nel settore della Sicurezza, con lo sviluppo di applicazioni sicure su dispositivi mobili, la sperimentazione di infrastrutture digitali per la sicurezza, sicurezza e crittografia, Digital Forensics.