# Soluzioni sicure per l'Internet of Things

La Commissione sta lavorando per garantire quadri di sicurezza piÃ¹ solidi e resilienti per i dispositivi IoT e le reti di cui fanno parte.

Â© iStock by Getty Images -1184401187 Jae Young Ju

I dispositivi Internet of Things (IoT) svolgono un ruolo chiave nel garantire la resilienza delle reti e nel mantenere i dati privati e sicuri. Tuttavia, la crescente tendenza nella complessitÃ  delle minacce alla sicurezza informatica comporta la necessitÃ  di framework di sicurezza piÃ¹ solidi per i dispositivi e le reti IoT.

Per affrontare questo problema, nel dicembre 2020 la Commissione europea ha presentato una strategia globale in materia di cibersicurezza per il decennio digitale, che delinea un percorso verso un'Internet diffusa delle cose sicure.

Il cluster di sicurezza dei progetti IoT affronta le carenze di dispositivi e reti. Lo fa sviluppando quadri sicuri e modulari che possono essere integrati in soluzioni nuove ed esistenti per la vita assistita, l'assistenza sanitaria, la produzione, l'approvvigionamento alimentare, l'energia e i trasporti. Questo cluster Ã¨ costituito da 8 progetti, per un importo di 40 milioni di EUR (circa 5 milioni di EUR ciascuno) in finanziamenti dell'UE.

Il cluster ha prodotto risultati degni di nota nei settori target. Sebbene le applicazioni siano specializzate, l'approccio di sviluppo modulare open-source utilizzato dai progetti consente di riutilizzare i moduli in altre soluzioni per un piÃ¹ ampio spettro di applicazioni.

## Progetti

### SecureIoT: Sicurezza predittiva per piattaforme IoT e reti di oggetti intelligenti

SecureIoT Ã¨ uno sforzo congiunto di leader globali nei servizi IoT e nella sicurezza informatica per garantire la prossima generazione di sistemi IoT decentralizzati. Questi spaziano su piÃ¹ reti di oggetti intelligenti, implementando una gamma di servizi di sicurezza aperti.

SecureIoT ha progettato servizi di sicurezza predittivi in linea con architetture di riferimento all'avanguardia per le applicazioni IoT, che servono come base per specificare i blocchi di sicurezza sia all'edge che al nucleo dei sistemi IoT. SecureIoT fornisce la raccolta, il monitoraggio e i

meccanismi predittivi dei dati di sicurezza, che offrono servizi integrati per la valutazione dei rischi, l'audit di conformitÃ  rispetto a regolamenti e direttive(regolamento generale sulla protezione dei dati, direttiva sulla sicurezza delle reti e dei sistemi informativi, direttiva ePrivacy) e supporto per gli sviluppatori.

I servizi di SecureIoT sono stati sfidati in scenari orientati al mercato in settori come la produzione intelligente e la mobilitÃ . Le loro implementazioni si basavano su servizi IoT apertamente disponibili e sulla comunitÃ  partner delle piattaforme. In un caso d'uso sulla vita intelligente, SecureIoT ha dimostrato il tempo necessario per rilevare gli attacchi nella robotica abilitata all'IoT. Con l'80Â % degli asset critici di questi robot socialmente assistivitrovati in una base di conoscenze sulla sicurezza, SecureIoT ha impiegato meno di 10 secondi per rilevare efficacemente le anomalie e meno di 5 minuti per una valutazione del rischio.

**Semiotica: InteroperabilitÃ , connettivitÃ  e sicurezza IoT di massa intelligente end-to-end**

Semiotics ha sviluppato un framework basato su modelli basati su piattaforme IoT esistenti per garantire un comportamento sicuro e semi-autonomico nelle applicazioni IoT industriali. Questi modelli hanno codificato le dipendenze tra sicurezza, privacy, affidabilitÃ  e interoperabilitÃ  dei singoli oggetti intelligenti.

Semiotica ha supportato l'adattamento cross-layer, inclusi oggetti intelligenti, reti e cloud, affrontando il comportamento autonomo a livello di campo (edge) e infrastruttura (backend). Per rispondere alle esigenze di complessitÃ  e scalabilitÃ  all'interno dei domini orizzontali e verticali, SEMIoTICS ha sviluppato meccanismi di networking programmabili e meccanismi di interoperabilitÃ  semantica. La sua praticitÃ  Ã¨ stata convalidata utilizzando tre casi d'uso nell'assistenza sanitaria, nelle energie rinnovabili e nel rilevamento intelligente.

Il consorzio Ã¨ composto da parti interessate dell'industria europea, delle PMI e del mondo accademico, che coprono l'intera catena del valore dell'IoT, l'analisi integrata locale e la loro connettivitÃ  programmabile al cloud con sicurezza e privacy.

**Mettere in atto DevOps**

Il movimento DevOps sostiene una serie di strumenti di ingegneria software per garantire una qualitÃ  del servizio e allo stesso tempo evolvere sistemi complessi e favorire cicli di innovazione rapidi e facilitÃ  d'uso. DevOps Ã¨ stato ampiamente adottato nel settore del software, ma oggi non esiste un supporto completo per sistemi IoT affidabili.

Implementa abilitatori di piattaforma consolidati per consentire DevOps nel regno di sistemi IoT affidabili, arricchendolo di sicurezza e resilienza, tenendo conto delle sfide legate all'attuazione collaborativa. Ha inoltre facilitato l'integrazione di questi concetti per sfruttare DevOps per piattaforme IoT esistenti e nuove come FIWARE, SOFIA e TelluCloud.

CiÃ² Ã¨ stato realizzato sviluppando le attuali tecniche DevOps per supportare il funzionamento dei sistemi IoT, fornendo una serie di meccanismi per garantire l'affidabilitÃ . Attraverso questo, ENACT ha fornito un framework DevOps per sistemi IoT intelligenti.

In un caso d'uso sul trasporto intelligente, ENACT ha valutato l'uso dell'IoT nel controllo dell'integritÃ dei treni. Qui l'infrastruttura e le risorse utilizzate sono costose e la pianificazione richiede molto tempo. L'utilizzo dei sistemi ferroviari Ã¨ stato ottimizzato, seguendo le direttive di sicurezza a causa delle caratteristiche critiche e strategiche del settore, assicurando il corretto trasporto di merci o passeggeri ed evitando eventuali incidenti.

Crawler di**IoT**

IOTCRAWLER

Lanciato nel febbraio 2018, IoTCrawler si Ã¨ concentrato sull'interoperabilitÃ  tra piattaforme, soluzioni riconfigurabili per l'integrazione di dati e servizi, algoritmi attenti alla privacy e sicuri e meccanismi per la scansione, l'indicizzazione e la ricerca nei sistemi IoT.

IoTCrawler ha fornito dimostrazioni con particolare attenzione all'Industria 4.0, alle comunitÃ  intelligenti e all'energia intelligente, fornendo un impatto attraverso la ricerca, l'innovazione e il progresso tecnologico. Il progetto ha affrontato sfide e problemi aperti nella scansione, scoperta, indicizzazione, integrazione semantica e sicurezza per un ecosistema IoT.

Il progetto ha effettuato il rilevamento dell'anomalia in un caso di utilizzo della gestione dell'acqua. L'analisi dei dati raccolti dai contatori intelligenti puÃ² personalizzare il feedback ai clienti, prevenire gli sprechi d'acqua e rilevare situazioni critiche. Nelle aziende di utilitÃ , il rilevamento delle anomalie viene spesso trascurato o fatto da un tecnico che non Ã¨ in grado di controllare tutti i metri a causa del volume di dati generati. In questo scenario, IoTCrawler ha esaminato due metodi per la rilevazione di anomalia serie temporali per vedere quali sono i piÃ¹ adatti per il consumo di acqua.

Il primo Ã¨ stato un framework basato su ARIMA (Auto Regressive Integrated Moving Average) che seleziona come punti che non si adattano a un processo ARIMA, e l'altro era la tecnica HOT-SAX (Heuristically Order Time series utilizzando Symbolic Aggregate Approximation), che rappresenta discretamente i dati e li discrimina utilizzando un euristico. Entrambi gli approcci si sono dimostrati efficaci nel rilevare le anomalie: Il 90Â % Ã¨ stato trovato utilizzando ARIMA e l'80Â % utilizzando HOT-SAX.

**Cervello-IoT: Framework basato su modelli per il rilevamento e l'attivazione affidabili nei sistemi IoT decentralizzati intelligenti**

Brain-IoT si Ã¨ concentrato su scenari in cui l'azionamento e il controllo sono supportati da sistemi IoT. L'obiettivo era quello di stabilire una metodologia a sostegno del comportamento cooperativo in federazioni componibili decentralizzate di piattaforme eterogenee.

Brain-IoT ha affrontato scenari business-critical e sensibili alla privacy soggetti a rigorosi requisiti di affidabilitÃ . In questo contesto, BRAIN-IoT ha permesso un comportamento autonomo intelligente che coinvolge sensori e attuatori che collaborano in compiti complessi. CiÃ² Ã¨ stato ottenuto impiegando piattaforme IoT, in grado di supportare operazioni sicure e scalabili per vari casi d'uso, supportate da un mercato aperto decentralizzato di piattaforme.

I modelli semantici aperti sono stati utilizzati per applicare operazioni interoperabili, scambiare dati e funzionalitÃ  di controllo, supportati da strumenti di sviluppo basati su modelli per facilitare la prototipazione e l'integrazione di soluzioni interoperabili. Le operazioni sicure sono state garantite da un framework che fornisce funzionalitÃ  AAA in scenari IoT distribuiti, uniti a soluzioni per incorporare la consapevolezza della privacy.

La fattibilitÃ  degli approcci Ã¨ stata dimostrata in due casi d'uso, vale a dire la robotica dei servizi e la gestione critica delle infrastrutture, nonchÃ© attraverso varie dimostrazioni proof-of-concept in collaborazione con iniziative pilota su larga scala.

## SOFIE: Federazione aperta sicura per Internet ovunque

Il progetto SOFIE ha creato un'architettura e un framework federativi sicuri e aperti. Ha utilizzato tecnologie di registro distribuito per consentire l'attuazione, la verificabilitÃ , i contratti intelligenti e la gestione delle identitÃ  e delle chiavi di crittografia. CiÃ² ha permesso soluzioni decentralizzate con scalabilitÃ  quasi illimitata.

Sofie ha affrontato la frammentazione dell'IoT attraverso la federazione, dove qualsiasi piattaforma IoT potrebbe unirsi creando un adattatore. I dati sono rimasti nelle piattaforme ed erano utilizzabili da tutte le applicazioni entro i limiti stabiliti dalle politiche di sicurezza. Il progetto ha esercitato la privacy fin dalla progettazione, fornendo sicurezza end-to-end, gestione delle chiavi, autorizzazione,

responsabilitÃ  e verificabilitÃ . L'utente potrebbe mantenere il controllo sui propri dati anche dopo che i dati sono stati memorizzati nel cloud conforme al GDPR.

Sofie ha lavorato su standard aperti, interfacce e componenti esistenti, come FIWARE, W3C Web of Thingse oneM2M, selezionando i componenti esistenti, sviluppandone di nuovi e raccogliendoli in un quadro per creare piattaforme aziendali gestite, aperte e sicure.

Sofie ha dimostrato la praticitÃ  del loro approccio utilizzandolo in tre piloti in tre diversi settori: la catena alimentare, il gioco e i mercati dell'energia. Per i piloti sono state realizzate tre piattaforme aziendali e i risultati sono stati valutati sulla base degli indicatori chiave di performance.

**Carro: Architettura cognitiva eterogenea per l'IoT industriale**

Charriot ha fornito una piattaforma di cognitive computing per supportare un approccio unificato verso la privacy, la sicurezza e la sicurezza dei sistemi IoT.

Tre siti pilota ad Atene (Grecia), Dublino (Irlanda) e Venezia (Italia) hanno dimostrato soluzioni realistiche attraverso implementazioni di riferimento del settore, con l'obiettivo di dimostrare che gli imperativi IoT sicuri, mediati dalla privacy e di sicurezza sono soddisfatti; un trampolino di lancio nella tabella di marcia dell'UE per le piattaforme IoT di prossima generazione.

CosÃ¬ come le minacce fisiche come gli atti di terrorismo, gli aeroporti stanno diventando sempre piÃ¹ vulnerabili alle minacce informatiche, che in futuro potrebbero sostituire il terrorismo fisico o essere combinati durante un attacco. Attacchi informatici e fisici combinati agli aeroporti potrebbero avere conseguenze devastanti. Le infrastrutture ICT tradizionali come server, desktop e reti utilizzate negli aeroporti sono collegate ad altri sistemi utilizzati in aree come i sistemi mission critical (maneggiamento bagagli, controllo ambientale, controllo accessi e controllo antincendio).

Il caso d'uso dell'aeroporto internazionale di Atene ha affrontato la sicurezza delle infrastrutture aeroportuali, aumentando la protezione delle strutture dalle minacce fisiche e informatiche. Carro ha migliorato la capacitÃ  dell'aeroporto di individuare precocemente e prevedere situazioni pericolose, in parallelo con la riduzione degli allarmi falsi positivi che interrompono le operazioni aeroportuali

Foto di**Seriot**

L'industria, le case e la societÃ  europee sperimentano i rischi per la sicurezza dell'IoT che accompagnano quotidianamente la tecnologia non testata. Gli attacchi ai contenuti e la qualitÃ  del servizio delle piattaforme possono avere conseguenze economiche, energetiche e fisiche che vanno oltre la tradizionale mancanza di sicurezza di Internet su computer e telefoni cellulari. Seriot Ã¨ stato fondamentale per implementare piattaforme e reti IoT sicure, ovunque e ovunque.

Il progetto ha sviluppato un framework IoT basato su una rete intelligente adattiva definita con router sicuri, analisi avanzate e analisi visiva user-friendly. Seriot ha ottimizzato la sicurezza delle informazioni nelle piattaforme e nelle reti in modo olistico e trasversale. I piloti hanno testato la tecnologia SerIoT in vari casi d'uso. Questi includono trasporti e sorveglianza intelligenti, produzione

flessibile all'interno dell'Industria 4.0 e altri settori emergenti come la logistica della catena alimentare, la m-Health e l'energia attraverso la rete intelligente. Attraverso questi sviluppi tecnologici e banchi di prova, il progetto ha fornito una rete software-based portatile unica in grado di guidare il successo dell'Europa nell'IoT.

Â

Segui gli ultimi sviluppi e scopri come partecipare.

- Seguire il lavoro della Commissione in materia di tecnologia e digitale @DigitalEU

## Ultime notizie

COMUNICATO STAMPA | 06 Dicembre 2022
L'UE investirÃ  13.5 miliardi di EUR in ricerca e innovazione per il periodo 2023-2024

La Commissione ha adottato oggi il principale programma di lavoro di Orizzonte Europa 2023-24, con circa 13.5 miliardi di EUR per sostenere i ricercatori e gli innovatori in Europa nella ricerca di soluzioni innovative per le sfide ambientali, energetiche, digitali e geopolitiche.

COMUNICATO STAMPA | 09 Febbraio 2022
Armonizzare lo spettro per migliorare la connettivitÃ : pronti per il 5G e l'innovazione

La Commissione ha adottato decisioni di esecuzione per garantire che la politica dell'UE in materia di spettro radio soddisfi la crescente domanda di banda larga e di applicazioni digitali innovative.

COMUNICATO STAMPA | 02 Febbraio 2022
Un nuovo approccio per una leadership mondiale dell'UE nel campo delle norme a favore dei valori democratici e di un mercato unico resiliente, verde e digitale

Questa settimana la Commissione ha presentato una nuova strategia di normazione che delinea il nostro approccio alle norme all'interno del mercato unico e a livello mondiale.

COMUNICATO STAMPA | 06 Settembre 2021
La Commissione pubblica uno studio sull'impatto di Open Source sull'economia europea

La Commissione ha pubblicato i risultati di uno studio che analizza l'impatto economico di Open Source Software e Hardware sull'economia europea.

Sfoglia @temi

## Contenuti correlati

### Quadro generale

La politica europea dell'Internet delle cose

L'UE coopera attivamente con l'industria, le organizzazioni e il mondo accademico per sfruttare il potenziale dell'Internet delle cose in tutta Europa e oltre.

### Vedere anche

L'Internet of Things di prossima generazione

Il futuro Internet of Things e Edge Computing possono rivoluzionare il modo in cui la produzione e i processi sono organizzati e monitorati attraverso catene del valore strategiche.

Mappatura dei cluster di innovazione dell'Internet of Things in Europa

Uno studio condotto sui cluster di Internet of Things (IoT) in Europa fornisce una comprensione piÃ¹ approfondita delle dinamiche, dei driver e dei fattori di successo in questo settore.

La digitalizzazione del settore agricolo europeo

La digitalizzazione del settore agricolo europeo ha il potenziale per rivoluzionare l'industria, promuovendo l'efficienza, la sostenibilitÃ  e la competitivitÃ .

---