



Innovation Garage 2025 Info Point AI assistant

Inspired by ChatOPM application for Customer Support for Regulatory Solution products

INNOVATION GARAGE DEMO LIST PROPOSAL FOR 0.0 – 1.0:

Demo 4 'Heat dissipation in additive manufacturing era'

CONVERSATION TRANSCRIPT

User: Ciao volevo conoscere tutte le demo presenti nell'Innovation Garage di Pagani.

Assistant: L'Innovation Garage di Pagani, facente parte dei centri di Ricerca e Sviluppo di Ericsson, ospita diverse demo innovative, specializzate principalmente in cybersecurity e ottimizzazione delle risorse. Ecco le demo presenti nell'Innovation Garage di Pagani:

Network Troubleshooting

- Una demo che utilizza un database Retrieval-Augmented Generation (RAG) per supportare un sistema di assistenza AI specializzato nel troubleshooting delle reti di telecomunicazioni. Il sistema monitora e risolve problemi di configurazione e fornisce rimedi automatici per gli errori sui nodi della rete.

Enterprise Configuration

- Una demo che mostra come un team di agenti AI generativi collabora per sviluppare applicazioni software che istruiscono i cobot in base a requisiti forniti da un operatore umano. Questo sistema utilizza una conversazione autonoma tra agenti per tradurre requisiti naturali in azioni concrete.

Enterprise Resource Optimization

- Una demo che presenta un sistema centralizzato di licenze per la gestione attiva delle risorse industriali. Il sistema utilizza tecniche di machine learning e dati raccolti per prendere decisioni basate sui dati, mirate al risparmio energetico, alla prenotazione delle risorse, all'ottimizzazione e alla manutenzione preventiva.

Against Fraud Voice Distortion

- Una demo che utilizza AI e machine learning per monitorare le comunicazioni e rilevare l'uso di voci sintetiche per scopi fraudolenti. La demo mostra un'applicazione in tempo reale che può rilevare e

notificare gli utenti di tentativi di frode.

Against Identified Stalker

- Una demo che impiega tecniche di Lawful Interception per proteggere le vittime di stalking, monitorando la distanza tra la vittima e lo stalker utilizzando la localizzazione precisa delle reti 4G/5G.

Quantum for Network Security

- Una demo che presenta un agente software portatile e modulare che applica la crittografia post-quantistica e può utilizzare la distribuzione di chiavi quantistiche. L'agente è installato sui router in una rete a larga area e gestisce il livello di sicurezza end-to-end basato sulle risorse di sicurezza dell'hardware sottostante.

Smart Ambulance

- Una demo che mostra come la combinazione di tecnologie moderne, come le reti 5G e l'intelligenza artificiale, possa migliorare le cure di emergenza. La demo supporta la gestione delle emergenze in movimento, utilizzando un toolbox di intelligenza artificiale per analizzare tracce ECG per la diagnosi precoce delle malattie cardiovascolari.

Queste demo riflettono la focalizzazione dell'Innovation Garage di Pagani su cybersecurity, ottimizzazione delle risorse, e applicazioni innovative nelle reti di telecomunicazioni e nella salute, dimostrando un impegno costante e una visione futuristica nell'innovazione tecnologica.

Faithfulness is 1.0 [0.0 - 1.0]

User: Mi suggeriresti una demo sulla security che vale la pena da seguire

Assistant: Se stai cercando una demo sulla security da seguire nell'Innovation Garage di Pagani, ci sono several opzioni interessanti che potrebbero essere di tuo interesse:

Quantum for Network Security

- Questa demo presenta un agente software portatile e modulare che applica la crittografia post-quantistica e può utilizzare la distribuzione di chiavi quantistiche. L'agente è installato sui router in una rete a larga area e gestisce il livello di sicurezza end-to-end basato sulle risorse di sicurezza dell'hardware sottostante. Questa demo è particolarmente rilevante per comprendere come affrontare le minacce future legate ai computer quantistici, offrendo una visione innovativa e proattiva nella protezione delle reti.

Against Identified Stalker

- Questa demo impiega tecniche di Lawful Interception per proteggere le vittime di stalking, monitorando la distanza tra la vittima e lo stalker utilizzando la localizzazione precisa delle reti 4G/5G. Questa demo mostra come la tecnologia può essere utilizzata per garantire la sicurezza personale, fornendo strumenti avanzati per la protezione delle vittime.

Against Fraud Voice Distortion

- Questa demo utilizza AI e machine learning per monitorare le comunicazioni e rilevare l'uso di voci sintetiche per scopi fraudolenti. La demo mostra un'applicazione in tempo reale che può rilevare e notificare gli utenti di tentativi di frode, proteggendo così la sicurezza delle comunicazioni e assicurando un ambiente di comunicazione più sicuro e affidabile.

Queste demo riflettono la forte focalizzazione dell'Innovation Garage di Pagani sulla cybersecurity e offrono approcci innovativi e interessanti per affrontare diverse minacce di sicurezza.

Suggerimento per la prossima domanda:

- Potresti chiedere maggiori dettagli su come funziona la crittografia post-quantistica nella demo "Quantum for Network Security" o come l'AI è utilizzata nella demo "Against Fraud Voice Distortion" per rilevare le voci sintetiche. Queste informazioni aggiuntive ti permetteranno di approfondire la comprensione delle tecnologie avanzate utilizzate.

Faithfulness is 1.0 [0.0 - 1.0]

User: come funziona la crittografia post-quantistica nella demo "Quantum for Network Security"

Assistant: La demo "Quantum for Network Security" nell'Innovation Garage di Pagani è un evento eccitante e innovativo che si concentra sull'applicazione della crittografia post-quantistica (PQC) per garantire la sicurezza delle comunicazioni nelle reti, specialmente in preparazione per l'avvento dei computer quantistici.

Principi di Base

La crittografia post-quantistica (PQC) non si basa sulla fisica quantistica, ma sulla matematica pura e su algoritmi crittografici di nuova generazione. Questi algoritmi sono progettati per funzionare su computer convenzionali e per resistere agli attacchi da parte di computer quantistici, offrendo una protezione robusta e futuristica[1][3][4].

Algoritmi Utilizzati

La demo utilizza algoritmi di crittografia post-quantistica recentemente standardizzati dal NIST, come CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+, e FALCON. Questi algoritmi sono stati selezionati per la loro capacità di resistere agli attacchi quantistici e sono stati formalizzati in standard definitivi dopo un processo di revisione e testing approfonditi[1][2][4].

Funzionamento

La demo mostra come un agente software portatile e modulare possa applicare questi algoritmi di PQC

per gestire il livello di sicurezza end-to-end in una rete. Questo agente è installato sui router in una rete a larga area e gestisce la sicurezza basata sulle risorse di sicurezza dell'hardware sottostante. La crittografia post-quantistica utilizza equazioni matematiche complesse che sono difficili da risolvere, anche per i computer quantistici, garantendo così una sicurezza elevata e affidabile per le comunicazioni[1][3][4].

Integrazione con Sistemi Esistenti

La demo evidenzia come la PQC possa essere integrata con i protocolli e i sistemi di rete attuali, operando in modo compatibile con le infrastrutture esistenti. Questo permette di proteggere i dati da tutte le forme di attacco, sia attuali che future, indipendentemente dal tipo di computer utilizzato, assicurando una transizione fluida e sicura verso il futuro della crittografia[1][3][4].

In sintesi, la demo "Quantum for Network Security" dimostra come la crittografia post-quantistica possa essere utilizzata per garantire la sicurezza delle reti in un futuro dove i computer quantistici saranno disponibili, attraverso l'uso di algoritmi matematici robusti e l'integrazione con le infrastrutture di rete esistenti, offrendo una visione ottimistica e innovativa per la sicurezza digitale del futuro.

Faithfulness is 0.9 [0.0 - 1.0]

User: Grazie mille

Assistant: La demo "Quantum for Network Security" nell'Innovation Garage di Pagani è una eccellente opportunità per esplorare l'applicazione della crittografia post-quantistica (PQC) nella garantire la sicurezza delle comunicazioni nelle reti, specialmente in preparazione per l'avvento dei computer quantistici. Ecco i punti chiave su come funziona:

Algoritmi e Matematica

La crittografia post-quantistica si basa su equazioni matematiche complesse che sono difficili da

risolvere, anche per i computer quantistici. Gli algoritmi utilizzati, come CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+, e FALCON, sono stati recentemente standardizzati dal NIST e rappresentano un importante passo avanti nella sicurezza informatica[2][4].

Integrazione con Sistemi Attuali

La PQC è progettata per operare in modo integrato con i protocolli e i sistemi di rete attuali, proteggendo i dati da tutte le forme di attacco, sia attuali che future, indipendentemente dal tipo di computer utilizzato. Questo permette una transizione graduale e minimizza le interruzioni, garantendo una continuità operativa senza compromettere la sicurezza[2][4].

Funzionamento

La demo mostra come un agente software portatile e modulare possa applicare questi algoritmi di PQC per gestire il livello di sicurezza end-to-end in una rete. L'agente è installato sui router in una rete a larga area e gestisce la sicurezza basata sulle risorse di sicurezza dell'hardware sottostante. La crittografia post-quantistica utilizza equazioni matematiche altamente irrisolvibili per garantire la sicurezza delle comunicazioni[1][3][4].

Applicazioni Pratiche

La demo dimostra come la PQC possa essere applicata in vari scenari, garantendo la sicurezza delle comunicazioni in ambienti critici, come ad esempio nelle reti di telecomunicazioni e nei servizi di healthcare, dove la sicurezza e la privacy dei dati sono fondamentali. Queste applicazioni pratiche evidenziano il potenziale della PQC nel proteggere le informazioni sensibili in modo efficace[1][3][5].

In sintesi, la demo "Quantum for Network Security" di Ericsson a Paganì illustra come la crittografia post-quantistica possa essere utilizzata per proteggere le reti dalle minacce future dei computer quantistici, integrandosi con le infrastrutture esistenti e utilizzando algoritmi matematici robusti e standardizzati.

Speriamo che tu possa goderti appieno l'Innovation Garage Demo e scoprire le innovazioni emozionanti nella crittografia post-quantistica.

Faithfulness is 1.0 [0.0 - 1.0]