AUTOMAZIONE OGGI AO

464
SETTEMBRE
2025 ANNO 42

SPECIALE
Gestione delle risorse energetiche

BECKHOFF

RASSEGNA
Sensori smart

PANORAMA
Digitalizzazione dei processi produttivi. A che punto siamo

TUTORIAL
Sensori quantistici

Quine EMPOWERING MINDS | SOLUZIONI SOFTWARE PER L'INDUSTRIA | Fieldbus & Networks | EMBEDDED

più intelligente e sostenibile, evitando gli elevati costi di emissione di CO_2 derivanti dalla costruzione di nuove strutture. La crisi energetica rappresenta una minaccia silenziosa per il settore dei data center: la domanda di energia è in forte crescita, spinta dai carichi di lavoro AI e dalle iniziative nazionali di trasformazione digitale. Tuttavia, l'infrastruttura di rete fatica a tenere il passo, rendendo obsoleta l'idea di una disponibilità energetica illimitata. Soluzioni di raffreddamento alternative e la sostituzione dei generatori diventano quindi essenziali.

Il futuro: investimenti, rendicontazione e il ruolo dell'AI

Il futuro del settore dei data center sarà sempre più indirizzato verso una trasformazione green, al fine di mitigare le emissioni di CO_2. Con l'entrata in vigore degli obblighi di rendicontazione sulla sostenibilità, come stabilito dalla direttiva Corporate Sustainability Reporting del Green Deal Europeo, le aziende dovranno necessariamente aumentare gli investimenti in questo settore. Una soluzione potrebbe riguardare la tecnologia basata sull'idrogeno, che garantirebbe ai data center di operare con energia pulita, rispettando l'ambiente e le richieste normative di net zero. Il report 'Powering the Future', realizzato da iXConsulting e BCS Consultancy, evidenzia una crescita costante della domanda di data center, con una previsione di triplicazione dei consumi energetici entro il 2030. L'85% degli intervistati ha registrato nell'ultimo anno un aumento della domanda legato all'AI, e l'87% prevede un'ulteriore crescita nei prossimi 12 mesi. Questo boom solleva preoccupazioni sulla capacità delle reti elettriche di gestire il crescente fabbisogno energetico e sulla disponibilità di energia rinnovabile. L'Italia ha il potenziale per diventare un hub strategico per i data center grazie alla sua posizione geografica e alle nuove infrastrutture, ma deve affrontare con urgenza la questione energetica e la formazione di personale qualificato. Considerando che il report sopracitato identifica la disponibilità di energia come fattore chiave per la localizzazione dei data center e la crescente domanda di energia rinnovabile, l'Italia deve sviluppare programmi di formazione mirati per colmare il divario di competenze. Solo affrontando queste sfide con una visione strategica di lungo termine, il nostro Paese potrà competere efficacemente a livello europeo e attrarre gli investimenti necessari per la crescita del settore. In conclusione, la gestione delle risorse energetiche è una sfida complessa che richiede un approccio olistico e una collaborazione tra operatori, governi e società civile. La sostenibilità non è solo un obiettivo da raggiungere, ma un imperativo per garantire un futuro prospero e sostenibile per il settore dei data center.

Powering the Future, realizzato da iXConsulting e BCS Consultancy

BCS Italia - https://bcsconsultancy.com/it

Foto Shutterstock

AI: come proteggerla? Come licenziarla?

Con l'aumento dell'adozione dell'intelligenza artificiale emergono nuove vulnerabilità, interrogativi e sfide legate alla protezione della proprietà intellettuale e alla gestione delle licenze

Daniela Previtali

L'intelligenza artificiale (IA) e le tecniche di machine learning (ML) stanno trasformando l'intero apparato digitale, di cui l'automazione industriale è uno dei principali pilastri. Dalla visione artificiale per il controllo qualità alla manutenzione predittiva, dall'ottimizzazione dei cicli produttivi alla gestione intelligente dell'energia, l'intelligenza artificiale è oggi un elemento strategico nella trasformazione digitale della fabbrica. Tuttavia, con l'aumento della sua adozione emergono nuove vulnerabilità, interrogativi etici e sfide legate alla protezione della proprietà intellettuale e alla gestione delle licenze.

Un potenziale da gestire in modo responsabile

Le reti neurali e gli algoritmi di deep learning sono progettati per replicare, seppur in forma limitata, il funzionamento del cervello umano. Tuttavia, a differenza degli esseri umani, un'AI non ha esperienze pregresse, intuizioni o buon senso. Lavora su insiemi di dati specifici e ottimizzati per attività come la classificazione, il riconoscimento, il rilevamento, la previsione, la segmentazione, il raggruppamento, la correlazione, l'ottimizzazione, la traduzione, la sintesi e la generazione. Un'AI non 'pensa' nel senso umano del termine. Non mette in discussione i dati in ingresso, né verifica autonomamente la validità del proprio output. Ciò significa che anche piccoli errori nei dati di training, intenzionali o accidentali, possono compromettere il comportamento del modello in modo imprevedibile. In contesti sensibili, una classificazione errata può avere conseguenze gravi. Le manipolazioni volontarie possono includere: l'inserimento di rumore visivo impercettibile per indurre una classificazione errata; l'etichettatura fuorviante di immagini o sequenze; la sostituzione selettiva di dati reali con dati sintetici generati ad hoc; l'alterazione del bilanciamento del dataset per favorire determinate risposte; l'iniezione di trigger nascosti (backdoor) in alcuni campioni; la modifica di metadati o marche temporali per falsare l'interpretazione temporale; la cancellazione sistematica di valori anomali (outlier) per ridurre la variabilità appresa dal modello. Un esempio classico è l'AI che apprende classificando 'sole' come 'gatto' e 'pioggia' come 'cane', ignorando del tutto l'animale raffigurato. Questo tipo di errore può diventare critico in contesti industriali safety-critical, dove una classificazione errata può danneggiare persone, macchinari o l'ambiente.

Il ciclo di vita del machine learning

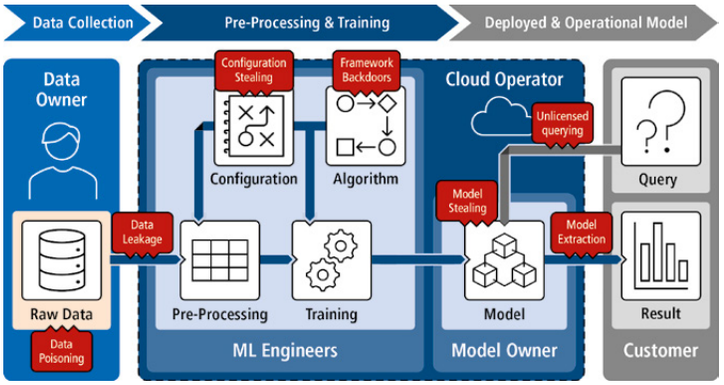
Per affrontare il problema alla radice, è necessario analizzare l'intero ciclo di vita del ML: un processo articolato che va dalla raccolta e preparazione dei dati grezzi, alla fase di addestramento, fino alla distribuzione del modello addestrato e al suo impiego in produzione.

- **Pre-processing dei dati:** Uniformare formati, risolvere incongruenze, ridurre le dimensioni o eliminare colonne irrilevanti.
- **Addestramento:** Il cuore del ciclo, dove l'algoritmo apprende le correlazioni presenti nei dati.
- **Distribuzione:** Il modello viene integrato in sistemi di produzione o prodotti software.
- **Inferenza e riaddestramento:** In alcuni casi, il modello continua a migliorarsi apprendendo anche dai dati operativi, generando però così anche nuovi punti di vulnerabilità, che vanno gestiti con la stessa cautela dei precedenti set di dati.

Ogni fase è suscettibile ad attacchi. La protezione deve essere quindi estesa a tutto il ciclo: dati, parametri, codice, algoritmi e modello finale.

Superfici di attacco e vulnerabilità

Le superfici d'attacco nel ML sono numerose: si va dalla manipolazione del dataset di training all'estrazione inversa del modello tramite attacchi black-box, fino all'inserimento di payload dannosi in input apparentemente innocui. Anche lo spionaggio industriale può trarre vantaggio da un accesso non autorizzato a modelli sofisticati, sottraendo anni di ricerca e sviluppo.
Inoltre, i modelli addestrati con dati sensibili (come immagini mediche, scansioni o informazioni personali) devono garantire la riservatezza sia in fase di addestramento che durante l'uso. Non si tratta solo di cybersecurity, ma anche di compliance normativa,



Superfici di attacco del ciclo di vita del machine learning

considerando, ad esempio, il rispetto degli obblighi previsti dall'AI Act europeo, entrato in vigore nel 2024 e applicabile a partire dal 2025 in forma graduale.

Wibu-Systems: protezione, licensing e conformità

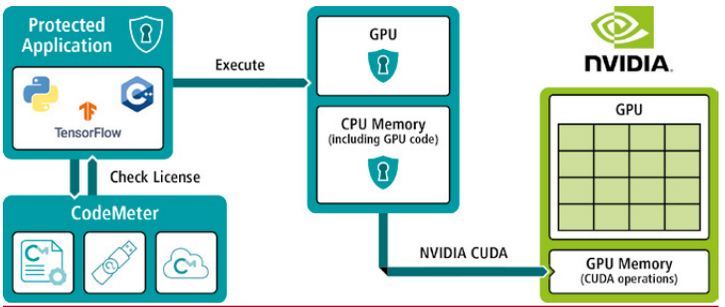
Da oltre 35 anni, Wibu-Systems sviluppa soluzioni avanzate per la protezione del software, la gestione delle licenze e la sicurezza informatica. Con la suite CodeMeter, è possibile proteggere applicazioni, dati e modelli AI contro reverse engineering, manipolazioni e usi non autorizzati. Il modulo AxProtector, in particolare, consente la cifratura e il controllo di accesso selettivo su file eseguibili e dati sensibili, incluse reti neurali e parametri di addestramento.

Una soluzione mirata è AxProtector Python, progettata per proteggere applicazioni AI scritte in Python, linguaggio diffuso per la facilità d'uso e l'ampia disponibilità di librerie di ML. AxProtector Python protegge sia il codice sorgente che i dati associati (dataset, modelli, parametri), applicando cifratura e integrità dei contenuti durante l'esecuzione.

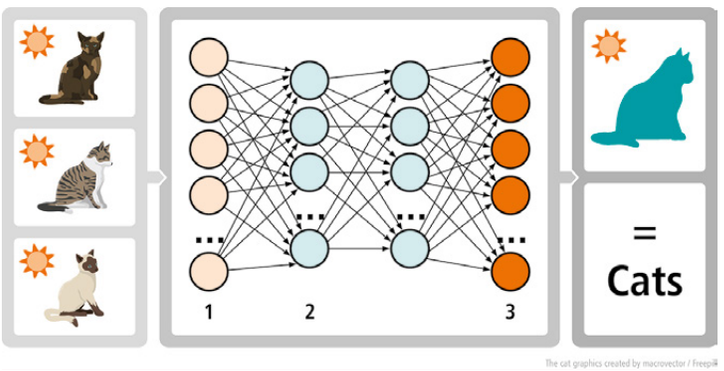
Grazie all'integrazione con CodeMeter License Central, è possibile gestire le licenze in cloud o in locale, anche per modelli distribuiti offline o su macchine isolate dalla rete. Le licenze possono essere temporanee, a consumo, vincolate a ruoli, ubicazioni o finestre temporali specifiche.

Ricerca applicata: il progetto Smile4KMU

Nel 2023 Wibu-Systems ha lanciato Smile4KMU, un progetto di ricerca cofinanziato dal Ministero tedesco per l'Istruzione e la Ricerca, con conclusione prevista per luglio 2026. L'obiettivo è fornire alle PMI tedesche soluzioni concrete per proteggere e licenziare modelli AI lungo tutto il loro ciclo di vita. In collaborazione con la Hochschule Offenburg e la start-up preML, il progetto studia casi d'uso legati al controllo qualità visivo in ambienti industriali. Tra le soluzioni esplorate ricordiamo la definizione di politiche di accesso e licenza già in fase di training; la protezione dei modelli con cifratura e controllo accessi in base alla granularità; la validazione dell'integrità del modello attraverso elementi hardware sicuri; la valutazione delle tecnologie di esecuzione riservata, come Nvidia Confidential Computing, che abilita l'esecuzione crittografata dei modelli direttamente sulla GPU.



Le operazioni all'interno della CPU, inclusa la memoria stessa della CPU, sono protette con CodeMeter



Superfici di attacco del ciclo di vita delCon dati di addestramento dell'AI non accuratamente selezionati, il modello risultante è inaffidabilemachine learning

Opportunità per il settore dell'automazione industriale

Il vantaggio competitivo si giocherà sempre di più sulla capacità di integrare l'AI in modo sicuro, trasparente e flessibile. Per i costruttori di macchine e per i fornitori di software industriale, questo significa abilitare modelli di licenza innovativi (ad esempio feature-on-demand), garantire la sicurezza dei modelli anche in ambienti ostili e rispondere in anticipo ai requisiti normativi in arrivo. In questo contesto, la protezione dell'AI non è solo una misura di sicurezza: è un catalizzatore per nuovi modelli di business. Le soluzioni di Wibu-Systems permettono alle aziende di industrializzare la propria AI, proteggere il know-how, mantenere la conformità normativa e monetizzare in modo sostenibile i propri investimenti in innovazione.

L'AI crea valore solo se è protetta

Proteggere il ciclo di vita dell'intelligenza artificiale è oggi una condizione imprescindibile per qualsiasi impiego industriale. L'adozione di tecnologie come CodeMeter consente, non solo di evitare violazioni e contraffazioni, ma anche di creare nuove opportunità di valore per le imprese. Con un quadro normativo in evoluzione ma in larga parte già delineato a livello europeo, e con l'AI sempre più pervasiva nella fabbrica intelligente, è arrivato il momento di agire.

Wibu Systems - www.wibu.com/it