ANNO OTTO NUMERO SEI - BIMESTRALE - NOVEMBRE/DICEMBRE 2024 - € 4,00

ÈUREKA!

INSIDE THE FUTURE

CRONACA DELL'INNOVAZIONE

COVER STORY
AI e software potenziano l'automazione di Mitsubishi Electric per facilitare la transizione digitale
p. 26

OPINIONI
Le strategie delle imprese nel formare nuove leve di tecnici. I manager illustrano idee e progetti
p. 72

SPECIALE IO-LINK
Le aziende del settore fanno il punto su tecnologie e trend per la comunicazione nella smart factory
p. 85

Poste Target Magazine LO/CONV/00388/02.2018 - P.I. 08/11/2024

ISSN 2704-808X

È! START

LA RIVOLUZIONE DELL'AI E LA SICUREZZA

▲ Nell'attuale panorama competitivo odierno, proteggere i propri modelli di intelligenza artificiale è una necessità.

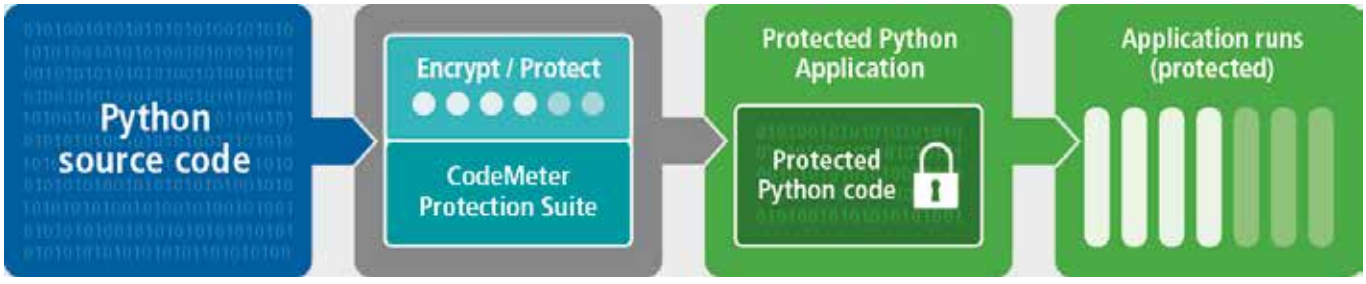
L'Intelligenza Artificiale (AI) è destinata a rivoluzionare ogni aspetto della nostra vita, dal lavoro alla quotidianità. In particolare, sempre più imprese adottano sistemi di Machine Learning per analizzare grandi quantità di dati, automatizzare i processi e sviluppare servizi altamente personalizzati. Ecco come Wibu-Systems mette in sicurezza l'insieme di tecnologie scaturite dalla digitalizzazione.

DI LUCIA QUAGLIETTA

Grazie alla sua semplicità e all'accesso a una vasta gamma di librerie specializzate come TensorFlow, PyTorch e Scikit-learn, Python fornisce una solida base per lo sviluppo di algoritmi AI complessi. Ma anche l'hardware gioca un ruolo cruciale. Con l'integrazione delle GPU (Graphics Processing Units), i programmatori Python possono addestrare modelli AI in modo più efficiente. Le GPU sono particolarmente adatte ai calcoli paralleli, comuni nei modelli di Machine Learning (ML). Questa capacità consente un'accelerazione massiva del processo di addestramento, particolarmente critica per set di dati di grandi dimensioni e modelli complessi. Allo stesso tempo, soluzioni hardware specializzate come le TPU (Tensor Processing Units) e gli FPGA (Field-Programmable Gate Arrays) stanno acquisendo sempre maggiore importanza. Questi dispositivi sono progettati per massimizzare le prestazioni dei sistemi AI, riducendo i tempi di calcolo e il consumo energetico.

In questo scenario, le aziende che investono nello sviluppo di algoritmi e modelli di AI devono garantire che i loro beni proprietari siano protetti per mantenere il loro vantaggio competitivo. Questa preoccupazione si estende non solo agli algoritmi stessi, ma anche all'implementazione di tali algoritmi in Python o C++ e ai dati sensibili di addestramento utilizzati per creare i modelli.

Purtroppo, il codice sorgente e i mo-



▲ La funzione fondamentale di AxProtector Python è proteggere e integrare le licenze nelle applicazioni Python.

delli addestrati sono generalmente facilmente accessibili. Ad esempio, gli script Python sono disponibili in testo semplice, il che li rende facili da visualizzare e analizzare.

Qui entra in gioco AxProtector Python, un prodotto progettato specificamente per proteggere il codice Python e i modelli di AI. Con AxProtector Python, le aziende possono crittografare e firmare il loro codice Python, assicurandosi che possa essere eseguito solo da utenti autorizzati e garantendo l'integrità del codice stesso. La modalità di crittografia dei file di AxProtector Python consente inoltre la crittografia sicura dei modelli di AI.

Negli ambienti nativi, dove le applicazioni AI sono sviluppate in linguaggi come C++, o i modelli vengono trasformati in codice nativo utilizzando LLVM, AxProtector Compile Time Protection (CTP) offre una soluzione completa per l'offuscamento, la crittografia e la firma. Questa tecnica altera il codice per renderlo illeggibile agli esseri umani, fornendo una protezione essenziale contro il reverse engineering e gli accessi illeciti.

L'importanza crescente dell'AI in vari settori sta portando a una maggiore regolamentazione. Quadri normativi, come l'AI Act e il Cyber Resilience Act (CRA) dell'UE, richiedono alle aziende di garantire che i loro sistemi di AI siano non solo efficienti ma anche sicuri. In particolare, i sistemi di AI ad alto rischio devono soddisfare rigorosi requisiti di sicurezza, per essere protetti da accessi non autorizzati e da manipolazioni.

Prodotti come AxProtector Python e AxProtector CTP aiutano le aziende a rispettare queste richieste normative. AxProtector Python protegge i modelli di AI e gli script Python tramite crittografia e ne garantisce l'integrità con firme digitali. AxProtector CTP fornisce meccanismi di protezione simili per applicazioni native e modelli trasformati tramite LLVM. Entrambe le soluzioni aiutano a soddisfare i requisiti del Cyber Resilience Act, in particolare nelle aree di riservatezza, integrità e disponibilità (CRA Allegato 1, Sezione 1.3 b, c e d), nonché le disposizioni dell'AI Act dell'UE.