UNIVERSITÀ DEGLI STUDI DI MILANO

La Statale a Expo 2020 Dubai con il progetto PALM su AI e cybersecurity

Presentato all'Expo 2020 Dubai il progetto PALM: proteggere e rafforzare i modelli di machine learning e intelligenza artificiale da attacchi avversariali e che mirano a manipolarne il funzionamento verso l'apprendimento di comportamenti errati

Dubai, 29 ottobre 2021. **L'apprendimento automatico (*machine learning*) e l'Intelligenza artificiale sono sempre più alla base del funzionamento dei sistemi distribuiti moderni.** Tali tecnologie accrescono l'intelligenza e l'autonomia dei sistemi e dei dispositivi che li compongono – dai robot alle telecamere, dalle apparecchiature mediche ai veicoli senza piloti o ai droni – e **sono diventati obiettivi privilegiati di attacchi che mirano a modificare il comportamento del sistema. Attacchi avversariali (*adversarial attack*) così come inquinamento e manipolazione dei dati (*poisoning*)** sono all'ordine del giorno e possono causare danni irreparabili ai modelli, ai sistemi e agli utilizzatori finali, mettendo a rischio l'incolumità stessa delle persone.

Il progetto ***Prevention and detection of poisoning and adversarial Attacks on Machine Learning Models*** (***PALM)*** scende in campo con l'obiettivo di **proteggere i sistemi e i loro utilizzatori finali da questi attacchi**, con l'obiettivo di supportare lo sviluppo e la messa in opera di sistemi sempre più robusti e affidabili. **PALM è un progetto internazionale che coinvolge l'Università degli Studi di Milano, l'Università di Roma "La Sapienza" e la Khalifa University of Science and Technology**, l'Ateneo più prestigioso degli Emirati Arabi Uniti, e che è stato **presentato a Expo 2020 Dubai durante l'evento del 28 ottobre** "*Connecting Safely, Creating the Future: Toward Securing Artificial Intelligence*" al Padiglione Italia.

Aumentare la robustezza e la resilienza dei modelli di machine learning, e in particolare delle tecniche di apprendimento automatico come il ***reinforcement learning***, è uno dei temi scientifici di interesse bilaterale individuati anche dal *Memorandum of Understanding* tra la Khalifa University, l'Università degli Studi di Milano e la Scuola Superiore Sant'Anna di Pisa.

Nel progetto PALM, gli Atenei partner lavorano allo sviluppo di un kit di strumenti migliorativi della resilienza e della robustezza dei modelli di apprendimento automatico che garantiscano immunità da *attacchi avversariali* e di manipolazione del processo di apprendimento. La soluzione proposta opererà a tre livelli: rafforzamento della fase di apprendimento dei modelli di *machine learning* attraverso la prevenzione da attacchi di manipolazione del dato, rafforzamento della fase di inferenza attraverso il rilevamento di modelli malevoli, attenuazione degli attacchi avversariali.

Ufficio Stampa Università Statale di Milano
Anna Cavagna - Glenda Mereghetti – Chiara Vimercati
tel. 02.5031.2983 – 2025 - 2982
ufficiostampa@unimi.it