a. 2020

Verona, 8 giugno 2020

Comunicato stampa

**L’ateneo di Verona tra i vincitori del Facebook awards 2020**

Il bando ha premiato l’idea di ricerca informatica tutta italiana sviluppata con Padova

**Studiare la vulnerabilità dei sistemi di intelligenza artificiale. Questo l’obiettivo alla base dell’idea di ricerca “Adversarial machine learning by morphological abstract interpretation” che giorni scorsi è risultata vincitrice del** [**2020 Probability and programming research awards**](https://research.fb.com/blog/2020/06/announcing-the-winners-of-the-2020-probability-and-programming-research-awards/)**, bando internazionale promosso da Facebook per premiare le migliori idee in materia di intelligenza artificiale e programmazione.**

**Autori della proposta di ricerca – unici italiani ad aver raggiunto il traguardo – sono Roberto Giacobazzi, direttore del dipartimento di Informatica dell’università di Verona, e Francesco Ranzato, docente di Informatica dell’ateneo di Padova.**

Da gennaio 2020 sono state raccolte 70 proposte di ricerca provenienti da oltre 51 università di 16 diversi Paesi. Tra i 19 vincitori del premio, il team italiano si è candidato con una ricerca sull’utilizzo di tecniche di analisi di programmi per studiare le vulnerabilità di sistemi di apprendimento automatico (machine learning), largamente impiegati in intelligenza artificiale.

“Esempi classici sono gli errori dei sistemi di intelligenza artificiale nel riconoscere oggetti, a volte causando incidenti anche catastrofici, ad esempio in sistemi a guida pienamente autonoma” spiega Roberto Giacobazzi. “Scopo della ricerca è evitare queste situazioni mediante tecniche formali - ossia matematicamente dimostrate - che riescano a garantire la corretta classificazione dentro specifici intervalli di tolleranza”.

“Le attuali tecniche di difesa sono spesso ad hoc e includono training sul modello con dati contraddittori, validazione degli input, e test della robustezza dei modelli. La nostra idea è invece **applicare tecniche di analisi automatica del software già sviluppate dal gruppo di ricerca** di Verona insieme ai colleghi dell’università di Padova, per garantire la correttezza del software a questo particolare problema”.

“In questo caso sfruttiamo una sorprendente quanto affascinante simmetria esistente tra i modelli utilizzati per l’analisi del software e quelli sviluppati per il filtraggio morfologico delle immagini” evidenzia Giacobazzi. “Questo significa codificare come astrazioni le perturbazioni morfologiche dei dati che possono causare errata classificazione, e utilizzare tecniche di interpretazione astratta per certificare la robustezza dei sistemi di classificazione rispetto a queste stesse perturbazioni”.

**Ufficio Stampa e Comunicazione istituzionale**

Telefono: 045.8028015 - 8717

M. 335 1593262

Email: [ufficio.stampa@ateneo.univr.it](mailto:ufficio.stampa@ateneo.univr.it)