SORS/WomenInBSC: Exploring Privacy Risk Exposure by Machine Learning

Objectives

Abstract: In recent years we are witnessing the diffusion of AI systems based on powerful machine learning models which find application in many critical contexts such as medicine, financial market, credit scoring, etc. In such contexts it is particularly important to design workflows for the learning of Trustworthy AI systems while guaranteeing interpretability of their decisional reasoning and privacy protection. In this talk we will explore the possible relationship between these two relevant ethical values to take into consideration in Trustworthy AI and how we can exploit machine learning for the assessment of privacy protection of data and (X)AI models.

Short bio: Anna Monreale is Associate Professor at the Computer Science Department of the University of Pisa and a member of the KDD LAB. Her research interests include big data analytics, decision making systems based on AI, machine learning and the study of privacy and ethical issues arising in learning AI models from these kinds of social

and human sensitive data. In particular, she is interested in the evaluation of privacy risks during analytical processes, in the definition of privacy-by-design technologies in the era of big data, and in the definition of methods for explaining black box decision systems. She earned her Ph.D. in Computer Science from the University of Pisa in June 2011 and her dissertation was about privacy-by-design in data mining.

This talk is co organized together with the Master in Artificial Intelligence (UPC,UB,URV).

Speakers

Speaker: Anna Monreale is Associate Professor at the Computer Science Department of the University of Pisa
Host: Prof. Ulises Cortés, High Performance Artificial Intelligence Group Manager, CS, BSC and Coordinator of the Master in Artificial Intelligence (UPC,UB,URV)

Barcelona Supercomputing Center - Centro Nacional de Supercomputación

---

Source URL (retrieved on *12 ago 2024 - 12:08*): https://www.bsc.es/ca/research-and-development/research-seminars/sorswomeninbsc-exploring-privacy-risk-exposure-machine-learning