UNIVERSIDAD
COMPLUTENSE
MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA
POSGRADO

Assessing machine learning systems from a security and trust standpoint

Robson de Oliveira Albuquerque
Universidad de Brasilia

Facultad de Informática
Aula 7 - miércoles 3 de julio de 2024 - 18:00
Entrada libre hasta completar el aforo

Resumen:

Machine learning systems have evolved incredibly in the last few years. Large language models are now common ground with different application scenarios. Startups are receiving an incredible amount of financing. But still, one main question remains: can we trust those systems for tasks that go beyond computationally repetitive tasks? Machine learning systems need labeled data, and for that data to make sense, it also needs context. If security is a necessary requirement, much of what is being said about machine learning systems won't stand any longer. This talk will provide you with a picture of the challenges that artificial intelligence faces and some interesting insights into the fields of security, machine learning, large language models, and trust.

Sobre Robson de Oliveira Albuquerque:

Robson de Oliveira Albuquerque received his Doctorate Degree from UnB in 2008 and got a PhD from UCM in 2016. In 2020 he finished his postdoc in cybersecurity at UnB in association with the professional postgraduate program in electrical engineering. He has more than 25 years of experience in computer networks, information systems and network security. His field of study and research includes Information Systems, Computer Networks, Network Security, Information Security and Cybersecurity. His professional skills include IT consulting for private organisations and the Brazilian Federal Government. He is a member of the Professional PostGraduate Program in Electrical Engineering (PPEE) in the Electrical Engineering Department, at the University of Brasília. He contributes as a Researcher and Professor at the Brazilian National Science and Technology Institute on Cybersecurity (CyberSecurity INCT) - LATITUDE Laboratory. He is member of AQUARELA research group at University of Brasilia. He has more than 50 international publications in journals and conferences related to computer science, computer networks, information security and cybersecurity.