ATRASS#9, October 15 2025

4pm CET , Patrick Gallinari, Criteo AI Lab, Paris and Sorbonne University

AI4Science: From Equations to Learning Machines

Abstract: This talk explores how **AI for Science** is transforming research across disciplines, shifting machine learning from a computational tool to a core scientific paradigm. The first part of the presentation briefly surveys examples from climate and weather forecasting, materials science, biology and drug discovery. The second part highlights, from a machine learning perspective, advances on modeling physical dynamical systems, emphasizing both the opportunities and the challenges of deploying machine learning in this field.

Bio : Patrick Gallinari is a professor at Sorbonne University, and a distinguished researcher at the Criteo AI Lab in Paris. His research focuses on statistical and deep learning with applications to semantic and complex data modeling. Since 2018, he has initiated research at the intersection of machine learning and physics, with a particular emphasis on spatio-temporal dynamics, and has contributed to seminal work in this field. He was awarded a national AI Chair (2020–2026) titled “Deep Learning for Physical Processes with Applications to Earth System Science,” and a second chair (2025–2031) titled “Deep Learning for Science: Modeling Fluid Dynamics in Engineering and Climate Physics.”

5pm CET : Shoaib Ehsan, University of Southampton

PRIV-LOC: Assessing and Mitigating Privacy Risks of Vision-Language Models in Image-based Geolocation Systems

Abstract: Vision-Language Models (VLMs) are increasingly demonstrating capabilities as image geolocators. These advanced AI models can infer sensitive location information from visual content, even when such information is not explicitly shared. With the integration of VLMs into social media platforms and other public-facing applications, the misuse of geolocation capabilities is no longer a theoretical concern but a pressing reality. For instance, millions of users upload images to social platforms

daily, often unaware that these images might inadvertently expose their private locations or sensitive contexts. The introduction of advanced AI models, such as Meta’s integration of LLaMA3-based AI into Facebook feed, highlights the immediacy of the risk, as these tools might allow both well-intentioned and malicious users to exploit geolocation capabilities at scale. The core problem lies in the dual-use nature of geolocation technologies. While they enable beneficial applications, such as improving disaster response, enhancing navigation, and geography education, they also create significant risks especially if the precision of such systems significantly improves in the future. These risks could lead to real-world harm, such as stalking, discrimination, or even threats to national security if sensitive infrastructures are revealed. In this talk, we will present our latest research findings (which were obtained as part of the PRIV-LOC project funded by the UK AI Security Institute) related to assessment and mitigation of these privacy risks of Vision-Language models in image-based geolocation systems. We seek to answer the crucial question: How can the privacy risks of VLM-powered geolocation systems be understood and minimized while maintaining their positive societal contributions? Our aim is to create actionable recommendations for the responsible development, deployment, risk assessment and governance of VLM-based geolocation systems. By balancing innovation with safety, it will help ensure these technologies are used in a trustworthy way while mitigating harmful outcomes.

Bio: Dr Shoaib Ehsan is an Associate Professor in the School of Electronics and Computer Science at the University of Southampton. He is also a Reader at the University of Essex. Dr Ehsan has a strong track record in Robotics and AI and has successfully led/co-led large UKRI research projects related to these fields (£46M funding in total). Currently, he is a Co-Investigator on the £33M Responsible AI UK programme, funded by UKRI/EPSRC. He is also leading the PRIV-LOC project funded by the UK AI Security Institute. Dr Ehsan is a winner of the British Machine Vision Association's Sullivan Doctoral Thesis Prize (2013), and was recognized as a 'Researcher with Exceptional Promise' by the Royal Academy of Engineering in 2014. He was awarded the prestigious IEEE Robotics and Automation Letters Best Paper - Honorable Mention Prize in 2025.

Video link

Microsoft Teams
: https://teams.microsoft.com/l/meetup-join/19%3ameeting_MThlMDg2ODAtODRlZS00NTdlLWFiYWYtNTlkYjI5NGI1NGQ2%40thread.v2/0?context=%7b%22Tid%22%3a%22efbb4c7c-8ac1-416d-bf30-791be86aad0b%22%2c%22Oid%22%3a%22c45eafbc-83c6-4d76-a89f-2c2450387d42%22%7d

ID de la réunion : 327 268 414 242 4
Code secret : QL2yk7tL