Department of Computer Science
香港城市大學
City University of Hong Kong

**COMPUTER SCIENCE COLLOQUIUM**

# Towards Securing Graph Neural Networks in MLaaS


SPEAKER **Prof Xingliang Yuan**

Associate Professor
School of Computing and Information Systems, University of Melbourne
Australia


DATE 11 Jun, 2024 (Tue)
TIME 10:30 AM - 11:30 AM
VENUE CS Seminar Room, Y6405, Yellow Zone, Yeung Kin Man Academic Building, City University of Hong Kong, Kowloon Tong, Hong Kong

## ABSTRACT


Graph Neural Networks (GNNs) extend the benefits of deep learning to graph data. In practice, their applications span from common utilities such as recommendation systems and fraud detection, to advanced domains such as drug discovery and physics simulation. Due to the increasing popularity of GNNs, commercial Machine Learning as a Service (MLaaS) platforms have integrated graph learning development tools for launching GNN services on the cloud, e.g., AWS integrated DGL, Microsoft Azure incorporated Spektral. Despite the convenience and low cost of model development and deployment, such graph-based MLaaS is also facing critical security challenges. In this talk, I will first overview the architecture of GNNs in MLaaS and elaborate on practical threats against privacy and integrity of GNNs. Then I will present our recent efforts in investigating and tackling those challenges. Along the line, I will also pinpoint open problems and future directions in this area.


## BIOGRAPHY

Xingliang Yuan is currently an Associate Professor in the School of Computing and Information Systems, the University of Melbourne. Before that, he was a faculty member at Monash University. He has a keen interest in designing systems to address privacy and security challenges in real-world contexts. His research has been supported by the Australian Research Council, CSIRO, Australian Department of Home Affairs, Australian Department of Health and Aged Care, and the Oceania Cyber Security Centre. His work has been published in major venues of computer security and systems, such as CCS, S&P, USENIX Security, NDSS, TDSC, TIFS, etc. He is a sole recipient of the Dean's Award for Excellence in Research by an Early Career Researcher (2020), and the Faculty Teaching Excellence Award (2021). He is a co-recipient of the best paper award in the European Symposium on Research in Computer Security 2021. He is on the editorial board of IEEE Transactions on Dependable and Secure Computing and IEEE Transactions on Service Computing. He is a track co-chair of ICDCS'24, WISE'24, MSN'24, PST'24, and program co-chair of SecTL'23 and NSS'22. He is a Senior Member of IEEE.

**All are welcome!**

*In case of questions, please contact Prof Cong WANG at congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at https://www.cs.cityu.edu.hk/events/cs-seminars/recent-cs-colloquiums.*