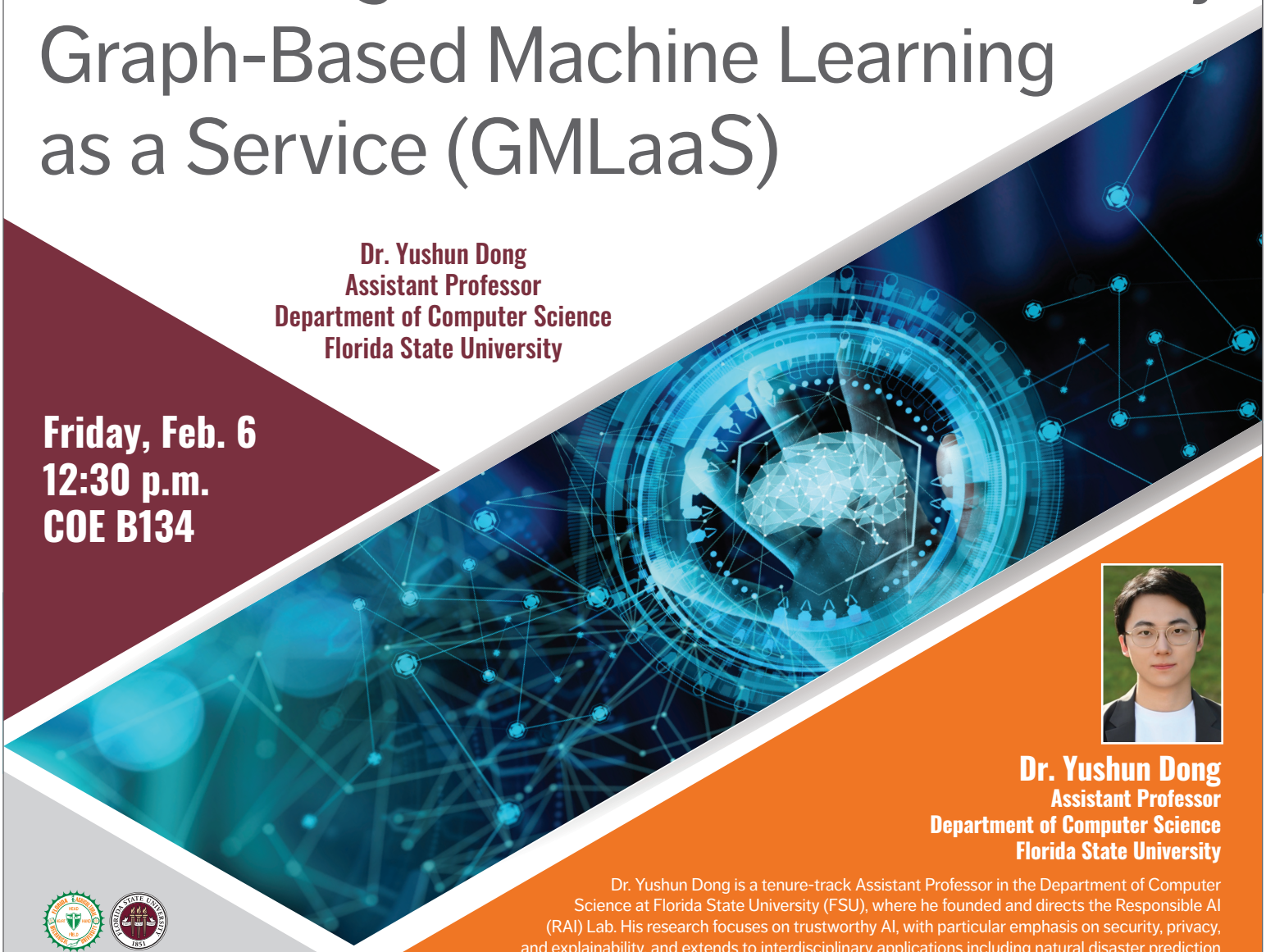
CIVIL & ENVIRONMENTAL ENGINEERING GRAD STUDENT SEMINAR ANNOUNCEMENT

Unleashing the Power of Trustworthy Graph-Based Machine Learning as a Service (GMLaaS)

Dr. Yushun Dong
Assistant Professor
Department of Computer Science
Florida State University

Friday, Feb. 6
12:30 p.m.
COE B134



Dr. Yushun Dong
Assistant Professor
Department of Computer Science
Florida State University

Dr. Yushun Dong is a tenure-track Assistant Professor in the Department of Computer Science at Florida State University (FSU), where he founded and directs the Responsible AI (RAI) Lab. His research focuses on trustworthy AI, with particular emphasis on security, privacy, and explainability, and extends to interdisciplinary applications including natural disaster prediction and resilience, healthcare, and social science. Dr. Dong serves as the lead Principal Investigator on multiple competitive research grants from major federal agencies, including the National Science Foundation, as well as internal research awards from Florida State University. His work has resulted in over 60 peer-reviewed publications in premier venues such as SIGKDD, NeurIPS, ICML, ICLR, WWW, and AAAI, with more than 1,900 citations and an h-index of 24. His research has been recognized with multiple honors, including the Best Short Paper Award at ACM SIGSPATIAL 2025, the Second Prize Award in the BlueSky Track at ICDM 2025, the Outstanding Doctoral Student Award and the Louis T. Rader Graduate Research Award from the University of Virginia, and the College of Arts and Sciences Dean's Faculty Award from FSU. Dr. Dong is also the creator of widely adopted open-source toolkits for trustworthy and graph-based machine learning, including PyOD V2 (over 32 million downloads and 9.4k+ GitHub stars), PyGDebias, and PyGIP, which have been broadly used in both academia and industry.

FAMU-FSU College of Engineering

This event is sponsored by
FAMU-FSU College of Engineering
Department of Civil & Environmental Engineering

Graph learning is increasingly delivered through Graph-based Machine Learning as a Service (GMLaaS) in many high-impact applications. While GMLaaS democratizes access to powerful graph learning models, this emerging service paradigm also introduces new fundamental challenges in trustworthiness.

This talk presents a coherent research landscape for trustworthy GMLaaS from three complementary perspectives. First, from the viewpoint of GMLaaS users, this talk presents methods that improve fairness, privacy, and explainability in graph learning, enabling reliable decision-making under real-world constraints. Second, from the perspective of GMLaaS model owners, this talk introduces techniques for understanding model stealing risks, monitoring against stealing attacks, and verifying model ownership, addressing emerging threats when graph learning models are exposed through APIs. Finally, this talk shows how these design principles drive impactful AI+X applications across AI4Science, AI4Geo, and AI4Healthcare. Together, the talk highlights how a service-oriented paradigm democratizes advanced AI capabilities by integrating trustworthiness into real-world deployments.