Computer Science Faculty Candidate

Phung Lai

Technical Presentation

Thursday, March 28 • 2 pm

Fisher 132 and Virtually

Talk Title: Trustworthy Machine Learning through the Lens of Privacy and Security

Talk Abstract: As machine learning (ML) is transforming our society, it is crucial to develop ML models that are not only accurate but also trustworthy (e.g., explainable, privacy-preserving, and secure), especially in critical applications such as healthcare, finance, etc. Achieving trustworthy ML with different learning paradigms and application domains is challenging, given the complicated trade-off among utility, scalability, privacy, explainability, and security. To bring trustworthy ML to real-world adoption, I developed a series of novel privacy-preserving mechanisms in which the trade-off between model utility and trustworthiness is optimized in different application domains, including natural language models, federated learning with human and mobile sensing applications, image classification, and explainable AI. The proposed mechanisms have reached deployment levels of commercialized systems in real-world trials while providing trustworthiness with marginal utility drops and rigorous theoretical guarantees. The developed solutions will enable safe, efficient, and practical analyses of rich and diverse user-generated data in many application domains.

Speaker Bio: Phung Lai is a Ph.D. candidate in Information Systems at the New Jersey Institute of Technology. Her research interests focus on trustworthy machine learning with the core of privacy and security. There are various applications, such as human sensing, mobile computing, healthcare, social goods, etc. Lai has authored 13 publications and some forthcoming work in the field. Her work has been published at leading venues, including AAAI, AISTATS, IEEE BigData, IEEE transactions, etc. In addition, Lai is a holder of several patents in privacy preservation in NLP. NSF and industrial partners, such as Adobe, Qualcomm, and Wells Fargo, have funded her work.

Use the QR code below to find the blog article and Zoom link.

Computing [MTU]
Department of Computer Science

1885 Michigan Tech