University of Pittsburgh | Informatics and Networked Systems
School of Computing and Information

You are receiving this email because you are enrolled in the MSIS/MST graduate degree programs within the Department of Informatics and Networked Systems at the School of Computing and Information. Each weekly newsletter will feature important updates on career/academic and job opportunities, department and school events, enrollment guidance and upcoming academic deadlines.

Spring Term Office Hours-Starting Tuesday, January 31, 2023:
Available in Person in IS Building Room 706
Tuesday: 2pm-4pm
Thursday: 11am-12pm or 1pm-2pm

Announcements

Spring 2023 In-Person Career + Internship Fair
(Open to all Pitt undergraduate and graduate students and alumni.)
February 16: Computing & Information
(Computer Science, Information Science, Computer Engineering and related majors and tech-/data-minded students.)11 a.m. - 3 p.m.

William Pitt Union

- **Registration opens at** noon on December 12.
- **Explore internship and full- and part-time employment opportunities.**
- **Meet with representatives from local, regional, and national nonprofits, corporations, and government agencies.**
- **Earn OCC credit.**
- **Wear professional attire (no jeans permitted).**
- **Bring plenty of resumes.**
- No pre-registration required.

Events

Dean's Spotlight Series: "Can We Make AI Foundation Models Secure, Private and Trustworthy?"

Wednesday, February 15 at 5:00 p.m. to 7:00 p.m.

130 North Bellefield Ave., Fifth Floor

Abstract: Foundation models refer to large machine learning models such as GPT-3 that promise to power the next generation of applications. Undoubtably their use will affect people's daily lives in meaningful ways. But are foundation models trustworthy and secure? These questions have recently captivated the attention of the technical community and general audience alike. There is speculation and uncertainty about their robustness, security, and privacy. Unfortunately, foundation models' large sizes and complexity are difficult to analyze to fully understand how trustworthy they are, and their typical black-box nature also adds a level of complexity. Over the past few years, I have studied the trustworthiness, security, and privacy of machine learning pipelines. In this talk, I will discuss how existing techniques to provide AI trustworthiness can in some instances be applied and how some fall short when considering foundation models, requiring new

methodologies. I will also discuss how recent research on privacy preserving federated learning can be sometimes at odds with the foundation model paradigm.

Bio: Nathalie Baracaldo leads the AI Security and Privacy Solutions team and is a Research Staff Member at IBM's Almaden Research Center in San Jose, CA. Nathalie is passionate about delivering machine learning solutions that are highly accurate, withstand adversarial attacks and protect data privacy. Her team focuses on two main areas: federated learning, where models are trained without directly accessing training data, and adversarial machine learning, where defenses are designed to withstand potential attacks to the machine learning pipeline. Nathalie is the primary investigator for the DARPA program "Guaranteeing AI Robustness Against Deception" (GARD). In 2020, Nathalie received the IBM Master Inventor distinction for her contributions to the IBM intellectual property and innovation. Nathalie also received the 2021 Corporate Technical Recognition, one of the highest recognitions provided to IBMers for breakthrough technical achievements to the Trusted AI Initiative, which has led to notable market and industry success for IBM. Nathalie co-edited the book "Federated Learning: A Comprehensive Overview of Methods and Applications" Springer, 2022. Nathalie received her Ph.D. degree from the University of Pittsburgh, USA in 2016.

RSVP here

DINS Seminar Series

Speaker: Isabella Loaiza, PhD student and Research Assistant, Human Dynamics Group, MIT Media Lab

February 15, 2023
11:00 am to 12 noon
Virtual -- more details to come!

You can find additional information on the DINS Seminar Series here: DINS Seminar Series: 2022-23 | Department of Informatics and Networked Systems | University of Pittsburgh

Career/Academic Opportunities

Women in Tech Breakfast Networking Reception: February 16, 2023

Hosted by SCI's DEI Committee & WiCS. Female, non-binary, and ally students are invited to a reception with corporate partners and friends of SCI. Pre-registration required here.

Application Developer (IT Application Development Journey)

Washington State Department of Ecology
On-site ·
Spokane, Washington, United State

Application deadline
March 27, 2023 3:00 AM

In this role, you would:

- Use advanced technical knowledge to develop statewide applications and maintain existing information systems (applications/databases) that agency staff, management, the regulated community, and the public rely on.
- Work with the IT team to perform analysis, system design, installation, maintenance, programming, quality assurance, troubleshooting, problem resolution, and consulting tasks for Hazardous Waste technical applications and databases.
- Use your excellent people skills to work directly with staff in an ongoing basis to determine requirements and make sure the data systems are working correctly.

The HWTR Program's mission is to protect Washington's residents and environment by reducing the use of toxic chemicals, safely managing dangerous waste, preventing new contaminated sites, and cleaning up contamination. The HWTR vision is to be national leaders in minimizing and eliminating the impacts of toxic chemicals and hazardous waste.

Application Developer (IT Application Development Journey) | Washington State Department of Ecology | Handshake (joinhandshake.com)

Enrollment Dates

February 13, 2023-Summer Term Open Enrollment Begins

For those planning on graduating in Spring of 2023 (otherwise known as term 2234 in PeopleSoft), you must apply to graduate to get your diploma (and, of course, successfully complete all appropriate coursework)!

Here is the timeline for Term 2234:

Graduation Application Opens – 10/1/22

Graduation Application Late Fee Begins – 12/1/22

Graduation Application Closes – 4/1/23

Final Day for ETD Paperwork & D-Scholarship Upload – 4/24/23

Please be advised that if you have not yet applied to graduate, you will be charged a $25 late fee. I would also be aware of the ETD Paperwork and D-Scholarship deadline (Complete Your Thesis or Dissertation | School of Computing and Information | University of Pittsburgh) if you are working on a Master's Thesis.

**********Please be advised, that if you have any questions, you can always reach out to me via the email and phone number below. **********

Regards,

James Petraglia (Pa-trail-ya)