VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Mohamed Elmahallawy
School of Engineering and Applied Science, WSU-TC

Does Space AI Security Matter?
Unlocking Privacy-Preserving Federated LEO Satellite Learning for Border Threat Detection

Oct. 8, 2024, 12:10 – 1 PM Pacific

Team Link: Click here to join the meeting
Meeting ID: 277 659 079 51| Passcode: WZ3ny7
Call in (audio only) +1 509-498-6399 | Phone conference ID: 986 879 057#

Abstract:

The rapid advancement of satellite technology has led to the deployment of microsatellites in low Earth orbit (LEO) that are equipped with high-resolution sensors and cameras capable of capturing vast amounts of Earth data. This data is used to train AI models for diverse applications, including climate monitoring, disaster response, agriculture, and border security. Federated learning (FL) offers a promising solution for maintaining privacy by enabling satellites to train models locally, without sharing sensitive data with centralized servers. However, sophisticated attackers have found ways to exploit model weights through techniques like membership inference and model inversion attacks, potentially reversing the private data used during training.

In this talk, we will explore cutting-edge techniques designed to secure these private models and protect data during transmission, even over insecure communication channels, ensuring robust privacy in the face of emerging threats.

Bio:

Mohamed Elmahallawy is a new Assistant Professor in the School of Engineering and Applied Science at Washington State University in the Tri-Cities campus. He previously served as a Postdoctoral Researcher in the Computer Science Department at Missouri University of Science and Technology. Dr. Elmahallawy earned his M.Sc. from the University of Rostock, Germany, in 2019, and completed his Ph.D. in Computer Science at Missouri University of Science and Technology, USA in 2024. Prior to his Ph.D., he worked as a Graduate Research Assistant in the Department of Electrical and Computer Engineering at Tennessee Technological University. His research interests encompass machine learning, federated learning, cryptography, network security, privacy preservation, and trustworthy AI. He explores applications in various domains, including low Earth orbit satellite networks, the Internet of Remote Things (IoRT), and medical applications.

cyser.wsu.edu