VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Dr. Upakar Bhatta
Assistant Professor, Central Washington University

Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Models

Feb. 3, 2026, 1:10 – 2 PM Pacific

Team Link: Click here to join the meeting
Meeting ID: 296 013 592 281 67| Passcode: KS69mu3T
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 855 422 642#

Abstract:

In today's AI-driven digital world, Governance, Risk, and Compliance (GRC) has become vital for organizations as they leverage AI technologies to drive business success and resilience. GRC represents a strategic approach that helps organizations using Large Language Models (LLMs) for automating tasks and enhancing customer service, while maintaining regulatory complexity across various industries and regions. However, LLM-driven systems introduce new forms of operational, ethical, and regulatory risk including data sensitivity exposure, and biased outputs can undermine operational integrity that must be addressed to ensure responsible AI deployment. This seminar explores a machine learning approach to evaluate GRC risks associated with LLMs. It utilizes Azure OpenAI Service logs to construct a representative dataset and train a model to predict GRC risk levels in LLM interactions, enabling organizations to improve efficiency, foster innovation, and deliver customer value while maintaining compliance and regulatory requirements.

Bio:

Dr. Upakar Bhatta joined CWU in September 2025 as an Assistant Professor in the ITAM department. Prior to that, he worked as an Adjunct Assistant Professor of cloud computing at University of Maryland Global Campus and an Assistant Teaching Professor at Arizona State University. He earned his D.Sc. degree in Cybersecurity from Marymount University in 2024. His expertise and research interests include the application of machine learning techniques to cybersecurity and cloud security domains. As part of his research, he has mentored students developing predictive models for risk assessment in multimodal AI systems, evaluated the effectiveness of integrating Zero Trust principles with Cloud-Native Application Protection Platforms (CNAPP), and identified Privacy Threshold Analysis (PTA) patterns to enhance data protection frameworks. Outside academia, he brings extensive hands-on experience in cloud infrastructure, networking, and cybersecurity. His corporate experience includes serving in various technical and leadership roles across government organizations at the city, state, and county levels. His positions have included Software Engineer, Cloud Security Specialists, Cloud Solution Architect, and Sr. Manager Systems/Network, where he contributed to enterprise infrastructure design, secure cloud migration strategies, and network optimization initiatives. In addition to his teaching and fieldwork, he holds several IT certifications, underscoring his commitment to excellence in both academic and applied domains.