Thesis Defense

Computer Science Master's Program

"Detecting Software Anomalies in Microservices Using Spectrograms, Scalograms, and Convolutional Neural Networks"

By **Snehith Jonnaikode**

Abstract:

The growing complexity of cloud-native microservices has intensified the need for robust anomaly detection mechanisms, particularly for misconfiguration-induced failures that propagate subtly across service boundaries. This thesis presents a runtime anomaly detection framework that transforms system metrics into frequency-domain representations—spectrograms (generated via the Short-Time Fourier Transform) and scalograms (derived from the Continuous Wavelet Transform)—and classifies them using Convolutional Neural Networks (CNNs). Evaluated on DeathStarBench, a production-grade microservices benchmark, the models target two injected misconfiguration anomalies affecting the Reservation and Recommendation services. To establish a baseline, Long Short-Term Memory (LSTM) models are trained on raw time-series features. CNNs trained on both spectrograms and scalograms consistently outperform the LSTM baselines, with the spectrogram-based CNN achieving a 93.77% F1-score, and the scalogram-based CNN attaining the highest overall performance: 98.54% accuracy, 98.53% F1-score, and a Matthews Correlation Coefficient of 0.9628. These results underscore the effectiveness of frequency-domain transformations for robust misconfiguration detection in dynamic microservice environments, laying the foundation for future research in multi-resolution modeling and real-time telemetry analysis.

Date: Friday, April 18th, 2025
Time: 3:00 PM – 5:00 PM
Zoom: https://calpoly.zoom.us/j/82922288457
Committee: Dr. Mukherjee, Dr. Mukhopadhyay, and Dr. Rwebangira