Thesis Defense

Computer Science Master's Program

"Towards Automated and Explainable Insider Threat Response in Electronic Health Records: A Role-Aware Machine Learning Framework"

By **Luca Lippi Ornstil**

Abstract:

Healthcare remains a prime target for cyberattacks, with insider misuse and credential compromise posing major risks to Electronic Health Records (EHRs). This thesis introduces a role-aware, explainable anomaly detection and response framework integrated with OpenEMR to address post-authentication threats. Four models—Local Outlier Factor (LOF), Isolation Forest, Autoencoder, and Graph Neural Network (GNN)—detect behavioral deviations across temporal, device, and role-based features, with LOF serving as the primary runtime detector. A configurable policy engine maps anomaly severity to proportional actions, from email alerts to read-only restrictions or account suspension, all reversible and auditable. Evaluation on real EHR logs shows the system's operational viability, balancing security automation with clinical continuity. The framework supports regulatory requirements while demonstrating that healthcare security can be both explainable and adaptive. It lays the groundwork for future multi-source anomaly detection and patient-safe cybersecurity automation in healthcare.

Date: Friday, November 14th, 2025
Time: 1:00 PM – 3:00 PM
Location: 14-238b
Committee: Dr. Fang, Dr. Debruhl, Dr. Matsumoto, Mr. Hoang Bao