Good Afternoon,
You are invited to attend our weekly ECE Graduate Seminar.

Old Dominion University
College of Engineering and Technology
Department of Electrical and Computer Engineering

All lectures to be held at 3:00pm on Fridays online at
https://vs.prod.odu.edu/kvs/zoom/?cid=202120_ECE731831GraduateSeminarSpring2022VS_96353
For more information, contact Dr. Chung Hao Chen at (757) 683-3475 or email cxchen@odu.edu.

Friday, March 4, 2022 Seminar Topic:

"Privacy Preserving Analytics to Enable Intrusion Detection Data Sharing" by Md. Ali Reza Al Amin, PhD student in the Computational Modeling and Simulation Engineering Department at Old Dominion University

Abstract:
Supervised learning is effectively adopted in Network Intrusion Detection Systems (IDS) to detect malicious activities in Information Technology (IT) and Operation Technology (OT). Sharing high-quality network data among cyber-security practitioners increases the chance to detect new threat campaigns by analyzing updated traffic features. As data sharing brings privacy concerns, Differential-Privacy (DP) has emerged as a promising approach to perform privacy-preserving analytics. This research develops a framework to generate high-quality synthetic network features using differentially private Generative Adversarial Network (DP-GAN). A well-known intrusion detection dataset, NSL-KDD, is used to conduct the experiments. To date, NSL-KDD has still been considered an intrusion detection benchmark because of its diverse attacks groups. The experiment records the classification performance of several machine learning (ML) models on a privacy-preserved synthetic dataset derived from the NSL-KDD intrusion dataset.

Bio:
MD ALI REZA AL AMIN received the M.S. degree in computer information and system engineering from Tennessee State University, Nashville, USA, in 2016. He is currently pursuing the Ph.D. degree in computational modeling and simulation engineering with Old Dominion University, Norfolk, USA. He has published numerous journals and conference papers. His research interests include but are not limited to Security and Privacy in Cyber Physical Systems, Machine Learning and AI in Security, Wireless Sensor Network, Internet of Things (IoT), and Data Science.