Postgraduate Seminar Series

Venue: Graduate Seminar Room
Date & Time: July 25, 2026 at 3:30 PM

Speaker Information

Kazi Samiul Kader (Std No. 1018052119) is a part time M.Sc. student in the department of CSE, BUET. He completed his undergraduate studies from BRAC University in 2015. His research interest lies in the field(s) of Cybersecurity, Machine Learning, and Deep Learning. He is currently doing his postgraduate thesis under the supervision of Dr. Md. Shohrab Hossain. He will be speaking about his ongoing research in this talk.

Geometric Label Flipping Attacks on Machine Learning-Based Ransomware Detection: A Distribution-Aware Analysis

Ransomware continues to inflict severe operational and financial damage, motivating the deployment of machine learning (ML) models for automated detection. These models depend on labeled training data, making them susceptible to label-flipping poisoning attacks. Prior work has explored random and boundary region flipping, but has not linked attack effectiveness to the geometric structure of the feature space or to the stealthiness cost imposed on the adversary. This thesis introduces the Compactness Index (CI), a geometric measure of class separation that predicts poisoning vulnerability at both the dataset and individual ransomware family level. We evaluate four label-flipping strategies — Random, Boundary, Center, and a novel Density-weighted Center variant — across three datasets and two classifiers. Using Maximum Mean Discrepancy to quantify detectability, we find that Boundary Attack achieves the best damage-to-stealthiness ratio, making it the adversary's strategically superior choice despite causing less raw damage than Center-based attacks. At the family level, higher compactness predicts greater resilience to poisoning. These findings show that ML-based ransomware detectors are vulnerable to simple, model-agnostic geometric poisoning, and motivate distribution-aware defenses.