

VINAYAK KOHLI

STUDENT, MASTER OF INFORMATION
SYSTEMS SECURITY AND ASSURANCE

DR. PAVOL ZAVARSKY

PROFESSOR, DEPARTMENT OF
INFORMATION SYSTEMS SECURITY
AND ASSURANCE MANAGEMENT



USING BINARY CLASS ANOMALY DETECTION TECHNIQUES TO PROTECT IOT DEVICES

The diverse environment of embedded devices used in the Internet of Things (IoT) creates unique problems in terms of detecting anomalies and responding to potential attacks. Recently attackers have deployed various techniques to utilize IoT devices to target critical infrastructures while avoiding detection. This research investigated methods to help prevent Distributed Denial of Service (DDOS) attacks, especially like those due to Mirai malware in 2016. We tested machine learning techniques to detect anomalies based on the analysis of IoT network behavior. In this paper, we created a binomial class, benign and anomaly dataset, on which various machine learning algorithms were tested. We also conducted a comparative analysis resulting in the identification of logistic regression as the most accurate algorithm in binary class anomaly detection.

***Research Advisor: Dr. Pavol Zavorsky,
Prof. Ron Ruhl***