Seminarium magisterskie II 2019/2020
Czasopismo: **IEEE Internet Of Things**
Tytuł: **Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things**
Link do artykułu**:** **https://ieeexplore.ieee.org/document/8693904**
Opracowanie: **Kamil Śladowski**
Autorzy artykułu:

Maede Zolanvari, Raj Jain, Lav Gupta - Department of Computer Science and Engineering, Washington University
Marcio A. Teixeira - Federal Institute of Education, Science and Technology of São Paulo
Khaled M. Khan - Department of Computer Science and Engineering, Qatar University

Zabezpieczenie urządzeń przemysłowych internetu rzeczy (IIoT) jest niezwykle ważne ze względu na potencjalnie katastrofalne konsekwencje w przypadku cyberataku. Do zwiększenia ich poziomu zabezpieczeń, stosowane są algorytmy uczenia maszynowego i analizy dużych zbiorów danych.

W artykule przedstawione zostały najpopularniejsze typy podatności i luk systemowych oraz zastosowanie ML w ich przeciwdziałaniu.

W badaniach, zaprezentowany został rzeczywisty system, zbudowany specjalnie do tego typu badań. Na nim to następnie przeprowadzono cyberataki i zaprojektowano narzędzia służące ich wykrywaniu.

W systemie zaimplementowano ‘backdoor’ i przygotowano sposób na dokonanie ‘code injection’. Następnie zademonstrowano jak system wykrywania anomalii, oparty na ML, może skutecznie radzić sobie w wykrywaniu tego typu ataków. Za pomocą znanych miar oceny jakości algorytmów, oceniono wydajność implementacji, by mieć właściwy punkt widzenia na skuteczność zastosowanych metod.

Przedstawione wyniki wskazują, że zastosowane uczenie maszynowe zadziałało dobrze w przeciwdziałaniu atakom cybernetycznym, mimo dużej dysproporcji danych użytecznych, do tych nieistotnych. Uważam że choć żaden system komputerowy nie będzie miał idealnych zabezpieczeń, to zastosowanie ML jeszcze lepiej wpłynie na ich bezpieczeństwo.