INTISARI

INSTRUSION DETECTION SYSTEM BERBASIS *ARTIFICIAL NEURAL NETWORK* DAN CT-GAN PADA JARINGAN INDUSTRI

Oleh:

Alvian Nur Azqy

21/473738/PA/20425

Penelitian ini mengatasi tantangan krusial keamanan siber pada sistem *Internet of Things* (IoT) dan *Cyber-Physical Systems* (CPS) yang rentan terhadap serangan canggih, terutama akibat ketidakseimbangan kelas dalam dataset pelatihan model deteksi intrusi (IDS) yang menyebabkan bias dan menurunkan efektivitas deteksi serangan minoritas.

Untuk itu, penelitian ini bertujuan mengembangkan dan mensimulasikan sistem IDS berbasis *machine learning* menggunakan *Artificial Neural Network* (ANN) yang didukung oleh data sintetis hasil *oversampling* dengan *Conditional Tabular Generative Adversarial Network* (CT-GAN) pada dataset CSE-CIC-IDS2018. Metode yang digunakan melibatkan pembuatan data sintetis oleh CT-GAN untuk menyeimbangkan kelas serangan minoritas, diikuti pelatihan model ANN menggunakan dataset yang telah diseimbangkan, serta simulasi jaringan industri dengan Raspberry Pi sebagai IoT Web Server dan CICFlowMeter untuk ekstraksi fitur lalu lintas.

Hasilnya menunjukkan bahwa CT-GAN berhasil menghasilkan data sintetis berkualitas tinggi (skor evaluasi mayoritas >80%, bahkan >96% untuk beberapa kasus) yang efektif menyeimbangkan distribusi kelas. Model ANN yang dilatih dengan data sintetis ini menunjukkan peningkatan kinerja signifikan, mencapai akurasi 89,47% dan AUC-PR 0, 9963, serta mampu mendeteksi berbagai serangan DoS dan *Brute Force* dalam 7-10 detik. Kesimpulannya, penggunaan CT-GAN terbukti efektif mengatasi ketidakseimbangan data dan meningkatkan kinerja model ANN secara signifikan, menghasilkan sistem IDS dengan kapabilitas deteksi cepat dan akurat, meskipun tantangan tetap ada pada serangan yang secara sintaksis mirip lalu lintas normal, yang mengindikasikan perlunya pengembangan lebih lanjut.

Kata kunci: Keamanan Siber, *Intrusion Detection System*, Machine Learning, Industri, CT-GAN, ANN

ABSTRACT

INTRUSION DETECTION SYSTEM BASED ON ARTIFICIAL NEURAL NETWORK AND CT-GAN IN INDUSTRIAL NETWORKS

By:

Alvian Nur Azqy

21/473738/PA/20425

This research addresses the crucial cybersecurity challenges in Internet of Things (IoT) and Cyber-Physical Systems (CPS) which are vulnerable to sophisticated attacks, primarily due to class imbalance in the training datasets of Intrusion Detection System (IDS) models, leading to bias and reduced effectiveness in detecting minority attacks.

Therefore, this study aims to develop and simulate an IDS based on machine learning using Artificial Neural Network (ANN) supported by synthetic data from oversampling with Conditional Tabular Generative Adversarial Network (CT-GAN) on the CSE-CIC-IDS2018 dataset. The methodology involves generating synthetic data using CT-GAN to balance minority attack classes, followed by training an ANN model with the balanced dataset, and simulating an industrial network with Raspberry Pi as an IoT Web Server and CICFlowMeter for traffic feature extraction.

The results indicate that CT-GAN successfully generated high-quality synthetic data (majority evaluation scores >80%, even >96% in some cases), effectively balancing class distribution. The ANN model trained with this synthetic data showed significant performance improvement, achieving 89,47% dan accuracy and 0, 9963 AUC-PR, and was capable of detecting various DoS and Brute Force attacks within 7-10 seconds. In conclusion, the use of CT-GAN proved effective in addressing data imbalance and significantly enhancing ANN model performance, resulting in an IDS with rapid and accurate detection capabilities, although challenges persist with attacks syntactically similar to normal traffic, indicating the need for further development with a hybrid detection approach.

Keywords: Cyber Security, *Intrusion Detection System*, Machine Learning, Industry, CT-GAN, ANN