Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem
Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Deteksi Serangan DdoS Pada Jaringan *Internet of Things* Menggunakan *Deep Learning* Sebagai Sistem Deteksi Intrusi

Daley Devlin Nugraha
22/504739/SV/21690

Perkembangan *Internet of Things* (IoT) meningkatkan kebutuhan terhadap sistem keamanan jaringan yang mampu mendeteksi serangan *Distributed Denial of Service* (DDoS) secara adaptif. Penelitian ini bertujuan merancang dan mengevaluasi *Intrusion Detection System* (IDS) berbasis *deep learning* untuk mendeteksi trafik normal dan serangan DDoS pada jaringan IoT, serta mengintegrasikan model terbaik dengan Bot Telegram sebagai media notifikasi otomatis. Dataset yang digunakan adalah CICDDoS2019 dengan klasifikasi multi kelas. Tahapan penelitian meliputi *preprocessing* data, penggabungan label, *feature engineering* menggunakan VarianceThreshold dan *correlation filtering* hingga diperoleh 52 fitur, normalisasi menggunakan RobustScaler, pembentukan *input sequence*, serta penanganan ketidakseimbangan kelas menggunakan *oversampling* dan *class weight*. Model yang diuji meliputi BiGRU, TCN, dan Hibrid TCN-BiGRU. Evaluasi dilakukan menggunakan *accuracy*, *Macro* F1-*Score*, *Balanced Accuracy*, MCC, ROC-AUC, *confusion matrix*, *classification report*, *learning curve*, dan waktu pelatihan. Hasil pengujian menunjukkan bahwa TCN memperoleh *accuracy* tertinggi sebesar 92,8739%, MCC 0,9118, dan ROC-AUC 0,9953 tetapi BiGRU dipilih sebagai model terbaik karena menghasilkan *Macro* F1-*Score* tertinggi sebesar 65,0824%, *Balanced Accuracy* 67,7829%, serta waktu pelatihan tercepat 20,7 menit. Implementasi BiGRU dengan Bot Telegram berhasil mengirimkan notifikasi hasil deteksi secara otomatis. Dengan demikian, BiGRU dinilai paling seimbang dari sisi performa, deteksi antar kelas, dan efisiensi waktu, meskipun kelas minoritas masih perlu ditingkatkan.

Kata Kunci: *Intrusion Detection System* (IDS), *Distributed Denial of Service* (DDoS), *Internet of Things* (IoT), *Deep Learning*, Bot Telegram

Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem
Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

DDoS Attack Detection in Internet of Things Networks Using Deep Learning as an Intrusion Detection System

Daley Devlin Nugraha
22/504739/SV/21690

The development of the Internet of Things (IoT) increases the need for a network security system capable of adaptively detecting Distributed Denial of Service (DDoS) attacks. This study aims to design and evaluate a deep learning-based Intrusion Detection System (IDS) to detect normal traffic and DDoS attacks on IoT networks, and integrate the best model with Telegram Bot as an automatic notification medium. The dataset used is CICDDoS2019 with multi-class classification. The research stages include data preprocessing, label merging, feature engineering using VarianceThreshold and correlation filtering to obtain 52 features, normalization using RobustScaler, input sequence formation, and handling class imbalance using oversampling and class weight. The models tested include BiGRU, TCN, and Hybrid TCN-BiGRU. Evaluation is carried out using accuracy, Macro F1-Score, Balanced Accuracy, MCC, ROC-AUC, confusion matrix, classification report, learning curve, and training time. The test results showed that TCN obtained the highest accuracy of 92.8739%, MCC of 0.9118, and ROC-AUC of 0.9953. However, BiGRU was chosen as the best model because it produced the highest Macro F1-Score of 65.0824%, Balanced Accuracy of 67.7829%, and the fastest training time of 20.7 minutes. The implementation of BiGRU with Telegram Bot successfully sent automatic notification of detection results. Thus, BiGRU was considered the most balanced in terms of performance, inter-class detection, and time efficiency, although the minority class still needs to be improved.

Keywords: Intrusion Detection System, DDoS, IoT, Deep Learning, Bot Telegram