Penerapan Metode Unsupervised Learning Autoencoder untuk Deteksi Lalu Lintas Botnet

ABSTRAK

Oleh : Rafi Ramadhan Ghifari, 202231013

Di bawah bimbingan Bapak Abdurrasyid, S.Kom., MMSI.

Perkembangan teknologi informasi dan komunikasi yang semakin pesat membawa dampak besar bagi berbagai aspek kehidupan manusia, mulai dari pertumbuhan ekonomi digital, efisiensi kerja, hingga transformasi layanan publik. Namun, kemajuan tersebut juga diiringi oleh meningkatnya ancaman keamanan siber. Salah satu ancaman yang cukup serius adalah serangan botnet, yaitu kumpulan perangkat yang terinfeksi malware dan dikendalikan oleh pihak tertentu untuk melakukan aktivitas berbahaya seperti pencurian data, spam, hingga serangan Distributed Denial of Service (DDoS). Sistem deteksi intrusi berbasis tanda tangan masih terbatas pada serangan yang sudah dikenal, sehingga dibutuhkan pendekatan berbasis anomali dengan metode unsupervised learning seperti autoencoder. Penelitian ini bertujuan untuk mengidentifikasi lalu lintas botnet menggunakan autoencoder. Data yang digunakan berasal dari dataset CIC-IDS-2018. Tahapan meliputi pra-pemrosesan data, pelatihan model autoencoder dan evaluasi model menggunakan metrik kuantitatif seperti accuracy, precision, recall, F1-Score, dan ROC-AUC. Hasil penelitian menunjukkan bahwa model autoencoder dengan normalisasi Standardization menghasilkan performa deteksi dengan nilai precision sebesar 88%, sehingga dapat membedakan antara lalu lintas normal dan botnet pada skema deteksi anomali.

Kata Kunci: *Botnet, Autoencoder, Unsupervised Learning, Deteksi Anomali, CIC-IDS 2018*

Application of the Unsupervised Learning Autoencoder Method for Botnet Traffic Detection

ABSTRACT

Authored by : Rafi Ramadhan Ghifari, 202231013

Under the Guidance by Mr. Abdurrasyid, S.Kom., MMSI.

The rapid development of information and communication technology has significantly impacted various aspects of human life, including the growth of the digital economy, work efficiency, and public service transformation. However, this advancement is also accompanied by an increase in cybersecurity threats. One of the most serious threats is a botnet attack, which consists of a group of devices infected by malware and controlled by certain parties to perform malicious activities such as data theft, spam, and Distributed Denial of Service (DDoS) attacks. Signature-based intrusion detection systems are still limited to known attacks, thus requiring an anomaly-based approach using unsupervised learning methods such as autoencoder. This research aims to identify botnet traffic using an autoencoder model. The data used in this study is sourced from the CIC-IDS-2018 dataset. The stages include data preprocessing, autoencoder model training, and model evaluation using quantitative metrics such as accuracy, precision, recall, F1-Score, and ROC-AUC. The results indicate that the autoencoder model with Standardization normalization method achieves detection performance by precision 88%, so that it can distinguish between normal traffic and botnets in the anomaly detection scheme.

Keyword: *Botnet, Autoencoder, Unsupervised Learning, Anomaly Detection, CIC-IDS 2018*