THRESHOLD PROFILING UNTUK DETEKSI SERANGAN DDOS MENGGUNAKAN DBSCAN PADA DATASET CIC-IDS2017

Nita Jariyah[1], Arief Ikhwan Wicaksono[2]

INTISARI

Latar Belakang: Serangan *Distributed Denial of Service* (DDoS) merupakan salah satu ancaman dalam keamanan jaringan yang dapat mengganggu ketersediaan layanan sistem. Deteksi serangan DDoS masih menghadapi tantangan signifikan, khususnya terkait tingginya kesalahan deteksi atau *false alarm.* Berdasarkan hal tersebut, diperlukan pendekatan deteksi yang mampu membedakan lalu lintas normal dan anomali pada serangan DDoS secara lebih akurat.

Tujuan: Penelitian ini bertujuan untuk mengembangkan sistem deteksi anomali serangan DDoS menggunakan pendekatan threshold profiling menggunakan algoritma DBSCAN pada dataset CIC-IDS2017.

Metode Penelitian: Penelitian ini menggunakan metode eksperimen dengan pendekatan Threshold-Based Detection. Data lalu lintas jaringan dari dataset CIC-IDS2017 diproses melalui tahapan *data cleaning*, *normalization*, dan *feature selection*, kemudian diklasterisasi menggunakan algoritma DBSCAN. Selanjutnya dilakukan perhitungan threshold berdasarkan distribusi statistik dari data normal. Setelah mendapatkan konfigurasi yang optimal, kemudian di evaluasi menggunakan metrik *Accuracy*, *Precision*, *Recall*, *F1-Score*, dan FPR untuk mengukur efektivitas deteksi.

Hasil: Sistem mampu mendeteksi anomali serangan DDoS dengan akurasi yang tinggi dan tingkat *false alarm* yang rendah. Algoritma DBSCAN berhasil membentuk klaster valid dari lalu lintas normal, dan threshold yang dihitung dari distribusi data benign mampu membedakan anomali dengan presisi yang baik.

Kesimpulan: Pendekatan threshold profiling berbasis algoritma DBSCAN efektif dalam meningkatkan akurasi deteksi anomali serta mereduksi *false alarm* dalam serangan DDoS. Sistem yang diimplementasikan dapat menjadi solusi untuk mendukung sistem keamanan jaringan.

Kata-kunci: Deteksi Anomali, DDoS, Threshold Profiling, DBSCAN, IDS, CIC-IDS2017

[1]Mahasiswa Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta
[2]Dosen Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta

THRESHOLD PROFILING UNTUK DETEKSI SERANGAN DDOS MENGGUNAKAN DBSCAN PADA DATASET CIC-IDS2017

Nita Jariyah[1], Arief Ikhwan Wicaksono[2]

ABSTRACT

***Background**: Distributed Denial of Service (DDoS) attacks are one of the major threats to network security, capable of disrupting system service availability. Detecting DDoS attacks still faces significant challenges, particularly in terms of high false alarm rates. Therefore, a detection approach is needed that can more accurately distinguish between normal and anomalous traffic in DDoS attacks.*

***Objective**: This research aims to develop an anomaly detection system for DDoS attacks using a threshold profiling approach with the DBSCAN algorithm on the CIC-IDS2017 dataset.*

***Method**: This research uses an experimental method with a Threshold-Based Detection approach. Network traffic data from the CIC-IDS2017 dataset undergoes data cleaning, normalization, and feature selection, followed by clustering using the DBSCAN algorithm. Thresholds are then calculated based on the statistical distribution of normal traffic. After obtaining the optimal configuration, the system is evaluated using metrics such as Accuracy, Precision, Recall, F1-Score, and False Positive Rate (FPR) to measure detection effectiveness.*

***Result**: The system is able to detect DDoS attack anomalies with high accuracy and a low false alarm rate. The DBSCAN algorithm successfully forms valid clusters from normal traffic, and the thresholds derived from the benign data distribution effectively distinguish anomalies with good precision.*

***Conclusion**: The threshold profiling approach based on the DBSCAN algorithm is effective in improving anomaly detection accuracy and reducing false alarms in DDoS attacks. The implemented system can serve as a potential solution to support network security systems.*

***Keywords**: Anomaly Detection, DDoS, Threshold Profiling, DBSCAN, IDS, CIC-IDS2017*

[1]Undergraduate Student of Information Technology, Faculty of Engineering and Information Technology, Universitas Jenderal Achmad Yani Yogyakarta
[2]Lecturer of Information Technology, Faculty of Engineering and Information Technology, Universitas Jenderal Achmad Yani Yogyakarta