KOMBINASI K-MEANS DAN DBSCAN DALAM MENDETEKSI ANOMALI JARINGAN PADA INTRUSION DETECTION SYSTEM (IDS)

Binta Aaliyah Hanifa[1], Alfirna Rizqi Lahitani[2]

INTISARI

Latar Belakang: Kemajuan teknologi informasi telah meningkatkan kompleksitas lalu lintas jaringan, sehingga mendeteksi serangan siber menjadi semakin menantang. *Intrusion Detection System* (IDS) dibutuhkan untuk mengidentifikasi aktivitas mencurigakan, namun sering menghadapi kendala dalam membedakan lalu lintas normal dan anomali. Untuk itu, diperlukan metode deteksi yang efektif dalam sistem keamanan jaringan.

Tujuan: Penelitian ini bertujuan untuk mengkaji efektivitas kombinasi algoritma K-Means dan DBSCAN dalam mendeteksi anomali jaringan, pada serangan DoS, pada sistem IDS.

Metode Penelitian: Metode yang digunakan adalah kombinasi algoritma K-Means dan DBSCAN secara *sekuensial*. K-Means digunakan untuk klasterisasi awal, sedangkan DBSCAN diterapkan untuk mendeteksi outlier sebagai anomali. Data yang digunakan adalah dataset UNSW-NB15, yang mencakup berbagai jenis serangan siber. Evaluasi dilakukan dengan *Silhouette Score* untuk mengukur kualitas *cluster* dan *False Positive Rate* (FPR) untuk menilai tingkat kesalahan deteksi.

Hasil: Hasil klasterisasi dengan K-Means menunjukkan nilai *Silhouette Score* tertinggi sebesar 0,8377 pada jumlah *cluster* terbaik k=4. DBSCAN berhasil mengidentifikasi 3.281 anomali dari total 16.353 data serangan DoS. Evaluasi menunjukkan FPR = 0, yang berarti tidak ada data normal yang salah terdeteksi sebagai serangan.

Kesimpulan: Kombinasi K-Means dan DBSCAN terbukti efektif dalam mendeteksi anomali pada IDS, dengan pemisahan *cluster* yang baik dan tingkat kesalahan deteksi yang sangat rendah.

Kata-kunci: *Intrusion Detection System*, K-Means, DBSCAN, Deteksi Anomali, DoS.

[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

KOMBINASI K-MEANS DAN DBSCAN DALAM MENDETEKSI ANOMALI JARINGAN PADA INTRUSION DETECTION SYSTEM (IDS)

Binta Aaliyah Hanifa[1], Alfirna Rizqi Lahitani[2]

ABSTRACT

***Background**: Advances in information technology have increased the complexity of network traffic, making cyberattack detection more challenging. An Intrusion Detection System (IDS) is essential for identifying suspicious activities, but often struggles to distinguish between normal and anomalous traffic. Therefore, an effective detection method is needed in network security systems.*

***Objective**: This study aims to evaluate the effectiveness of a combination of K-Means and DBSCAN algorithms in detecting network anomalies, specifically DoS attacks, within an IDS.*

***Method**: The method used is a sequential combination of the K-Means and DBSCAN algorithms. K-Means is used for initial clustering, while DBSCAN is applied to detect outliers as anomalies. The dataset used is UNSW-NB15, which includes various types of cyberattacks. Evaluation is conducted using the Silhouette Score to measure cluster quality and the False Positive Rate (FPR) to assess detection accuracy.*

***Result**: The K-Means clustering achieved the highest Silhouette Score of 0.8377 at the optimal number of cluster, k=4. DBSCAN successfully identified 3,281 anomalies out of a total of 16,353 DoS attack records. The evaluation showed an FPR of 0, indicating no normal data was mistakenly identified as an attack.*

***Conclusion**: The combination of K-Means and DBSCAN has proven effective in detecting anomalies in IDS, offering well-separated cluster and a very low error rate in detection.*

***Keywords**: Intrusion Detection System, K-Means, DBSCAN, Anomaly Detection, DoS.*

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