Abstrak

Intrusion Detection System (IDS) berperan sebagai pendeteksi berbagai jenis serangan pada jaringan komputer. IDS mengidentifikasi serangan berdasarkan klasifikasi data jaringan. Saat ini, beberapa metode klasifikasi IDS masih memiliki kekurangan dan kelebihan masing-masing. Salah satu permasalahan pada IDS adalah tingkat performa akurasi yang masih rendah. Beberapa faktor yang mempengaruhi performa akurasi IDS diantaranya pelatihan dataset yang sudah usang, ketidakseimbangan data latih dan pemilihan metode klasifikasi menjadi tantangan untuk penelitian ini. Dengan melakukan studi literatur pada klasifikasi non-IDS, ditemukan metode yang memilki performa klasifikasi baik, yaitu *AdaBoost*. Sedangkan untuk menangani ketidakseimbangan data, *Synthetic Minority Oversampling Technique* (SMOTE) menjadi salah satu cara untuk menangani permasalahan tersebut. *Principal Component Analysis* (PCA) dan *Ensemble Feature Selection* (EFS) dapat diterapkan sebagai pemilihan fitur pada dataset IDS. Sehingga metode-metode tersebut patut dianalisis performanya dalam klasifikasi data IDS untuk dapat mengatasi kekurangan metode sebelumnya. Oleh karena itu, pada tugas akhir ini kami mengusulkan beberapa skema untuk meningkatkan performa IDS pada dataset CIC 2017. Hasil empiris menunjukan bahwa pada klasifikasi *AdaBoost* menggunakan PCA dan SMOTE menghasilkan nilai AUC 92% dan pada klasifikasi *AdaBoost* menggunakan EFS dan SMOTE menghasilkan akurasi 81,83%, *precision* 81,83%, *recall* 100%, dan *F1 Score* 90,01% lebih tinggi dibandingkan dengan klasifikasi AdaBoost pada penelitian sebelumnya hanya memiliki nilai presisi 77%, *recall* 84% dan *F1 Score* 77%.

Kata Kunci: *Intrusion Detection System*, DDoS, AdaBoost, SMOTE, PCA.