ABSTRAK

DDoS merupakan salah satu bentuk serangan siber yang paling mengancam dan berbahaya di dunia. Serangan DDoS mampu menyebabkan kelumpuhan server milik korban yang mengakibatkan gangguan layanan yang mengarah pada kerugian moril dan ekonomi. Salah satu upaya pencegahan serangan DDoS adalah dengan menerapkan *Intrusion Detection System* (IDS) berbasis *Artificial Neural Network* (ANN). Akan tetapi, dalam proses pelatihan ANN pemilihan fitur berperan sangat penting dalam menentukan performa model. Penelitian ini mencoba untuk mengetahui pengaruh seleksi fitur gabungan *Information Gain* dan XGBoost terhadap performa model deteksi serangan DDoS yang menggunakan ANN. Proses seleksi fitur diterapkan pada dataset DDoS yang komprehensif yaitu UNSW-NB15. Hasil penelitian menunjukkan bahwa model ANN dengan lima fitur terpilih (sttl, dbytes, state, sbytes, smean) mencapai *accuracy* 0,902, *precision* 0,859, dan *recall* 0,959 tanpa indikasi *overfitting* atau *underfitting*. Apabila dibandingkan dengan model *baseline* (tanpa seleksi fitur), model ini memiliki recall lebih tinggi (+0,03) dan waktu komputasi lebih cepat (-12,23 detik), tetapi dengan konsekuensi *precision* yang lebih rendah (0,859 vs. 0,953). Hal ini menunjukkan bahwa seleksi fitur gabungan *Information Gain* dan XGBoost mampu meningkatkan efisiensi dan deteksi serangan DDoS (*recall*), tetapi mengorbankan skor *precision*, sehingga berpotensi meningkatkan *false positive* dalam klasifikasi lalu lintas jaringan.

Kata Kunci: DDoS; ANN; Seleksi Fitur; *Information Gain*; XGBoost.

ABSTRACT

Distributed Denial of Service (DDoS) is one of the most threatening and dangerous forms of cyberattacks worldwide. A DDoS attack can paralyze a victim's server, leading to service disruptions that result in both moral and economic losses. One preventive measure against DDoS attacks is the implementation of an Intrusion Detection System (IDS) based on Artificial Neural Networks (ANN). However, feature selection plays a critical role in determining the performance of ANN models during the training process. This study aims to investigate the impact of combining Information Gain and XGBoost feature selection methods on the performance of an ANN-based DDoS detection model. The feature selection process is applied to a comprehensive DDoS dataset, namely UNSW-NB15. The results indicate that the ANN model utilizing five selected features (sttl, dbytes, state, sbytes, smean) achieves an accuracy of 0.902, precision of 0.859, and recall of 0.959 without signs of overfitting or underfitting. Compared to the baseline model (without feature selection), the proposed model demonstrates a higher recall (+0.03) and faster computation time (-12.23 seconds), albeit with a trade-off in precision (0.859 vs. 0.953). These findings suggest that the combined use of Information Gain and XGBoost enhances detection efficiency and recall in identifying DDoS attacks, but at the cost of reduced precision, potentially increasing the false positive rate in network traffic classification

Keywords: DDoS; ANN; Feature Selection; Information Gain; XGBoost.