INTISARI

Serangan Denial of Service (DoS) merupakan ancaman utama bagi keamanan jaringan, hal ini ditandai dengan melimpahnya sumber daya sistem dengan permintaan yang tidak sah. Serangan yang demikian dapat mengganggu layanan-layanan penting dan menyebabkan kerugian finansial yang besar. Penelitian ini mengevaluasi efektivitas empat algoritma machine learning yaitu Random Forest, Linear Discriminant Analysis (LDA), Logistic Regression dan Naïve Bayes dalam mendeteksi serangan DoS dengan menggunakan dataset NSL-KDD sebagai standar. Penelitian ini bertujuan untuk menentukan algoritma yang paling dapat diandalkan untuk mendeteksi serangan DoS melalui analisis komparatif. Metodologi yang digunakan meliputi prapemrosesan data, pemilihan fitur, pengkodean label, dan penyeimbangan menggunakan SMOTE. Setiap algoritma tersebut dilakukan hyperparameter tuning dan validasi silang 10 bagian untuk mengoptimalkan kinerja. Metrik evaluasi seperti akurasi, presisi, recall, dan F1-score digunakan untuk perbandingan model. Hasilnya menunjukkan bahwa Random Forest mencapai akurasi tertinggi (99,97%) dan kinerja yang unggul di semua metrik, menunjukkan generalisasi dan presisi yang sangat baik. LDA, Logistic Regression dan Naïve Bayes juga memiliki kinerja yang baik tetapi tidak sebaik Random Forest dalam menangani pola yang kompleks dalam dataset. Penelitian ini menekankan pentingnya penggunaan teknik machine learning untuk deteksi intrusi jaringan, terutama dalam mengatasi ancaman DoS. Hasil penelitian ini memberikan wawasan yang bermanfaat untuk memilih algoritma yang sesuai untuk implementasi di masa depan dalam sistem keamanan siber.

Kata kunci: Denial of Service, Machine Learning, Keamanan Jaringan, Dataset NSL-KDD

ABSTRACT

Denial of Service (DoS) attacks are a major threat to network security, characterized by overwhelming system resources with illegitimate requests. Such attacks can disrupt critical services and cause substantial financial losses. This study evaluates the effectiveness of four machine learning alghorithms namely Random Forest, Linear Discriminant Analysis (LDA), Logistic Regression and Naïve Bayes in detecting DoS attacks using the NSL-KDD dataset as a benchmark. The research aims to determine the most reliable algorithm for detecting DoS attack through a comparative analysis. The metodology involves data preprocessing, feature selection, label encoding and balancing using SMOTE. Each algorithm underwent hyperparameter tuning and 10-fold cross validation to optimize performance. Evaluation metrics such as accuracy, precision, recall and F1-score were used for model comparison. Results indicate that Random Forest achieves highest accuracy (99,97%) and robust performance across all metrics, demonstrating superior generalization and precision. LDA, Logistic Regression and Naïve Bayes also performed well but fell short of Random Forest in handling complex patterns in the dataset. This research highlights the significance of employing machine learning techniques for network intrusion detection, particularly in addressing DoS threats. The findings provide valuable insights into selecting suitable algorithms for future implementations in cybersecurity systems.

Keywords: Denial of Service, Machine Learning, Network Security, NSL-KDD Dataset