

ABSTRAK

Distributed Denial of Service (DDoS) merupakan salah satu serangan siber yang dapat mengganggu ketersediaan layanan jaringan dengan membanjiri target menggunakan lalu lintas dalam jumlah besar. Penelitian ini bertujuan untuk mengimplementasikan algoritma Gaussian Naive Bayes dalam mendeteksi dan mengklasifikasikan trafik normal dan trafik serangan DDoS pada lingkungan Internet of Things (IoT) menggunakan dataset CICIoT2023. Data yang digunakan difokuskan pada kategori Benign Traffic dan DDoS-ICMP Flood. Tahapan penelitian meliputi pengumpulan dataset, preprocessing dan pembersihan data, pemisahan fitur dan label, pembagian data menjadi 80% data training dan 20% data testing, serta seleksi fitur menggunakan SelectKBest dengan metode Mutual Information. Dari fitur yang tersedia, dipilih 20 fitur terbaik untuk digunakan dalam proses klasifikasi menggunakan algoritma Gaussian Naive Bayes. Evaluasi model dilakukan menggunakan confusion matrix dengan parameter accuracy, precision, recall, dan F1-score. Hasil pengujian menunjukkan bahwa model Gaussian Naive Bayes memperoleh accuracy sebesar 62,96%, precision sebesar 42,05%, recall sebesar 99,53%, dan F1-score sebesar 59,12%. Nilai recall yang tinggi menunjukkan bahwa model mampu mengenali sebagian besar trafik yang merupakan serangan DDoS. Namun, nilai precision, accuracy, dan F1-score menunjukkan bahwa model masih menghasilkan kesalahan klasifikasi, khususnya dalam membedakan trafik normal dan trafik DDoS secara seimbang. Dengan demikian, algoritma Gaussian Naive Bayes pada penelitian ini memiliki kemampuan yang tinggi dalam mengenali trafik serangan DDoS, yang ditunjukkan oleh nilai recall sebesar 99,53%, namun masih memiliki keterbatasan dalam membedakan trafik normal dan trafik DDoS secara seimbang.

Kata kunci: *DDoS*, Gaussian Naive Bayes, *CICIoT2023*, *Machine Learning*, Deteksi Intrusi.

ABSTRACT

Distributed Denial of Service (DDoS) is one of the cyberattacks that can disrupt the availability of network services by overwhelming a target with a large amount of traffic. This study aims to implement the Gaussian Naive Bayes algorithm to detect and classify normal traffic and DDoS attack traffic in an Internet of Things (IoT) environment using the CICIoT2023 dataset. The data used in this study focuses on the Benign Traffic and DDoS-ICMP Flood categories. The research stages include dataset collection, preprocessing and data cleaning, feature and label separation, data splitting into 80% training data and 20% testing data, and feature selection using SelectKBest with the Mutual Information method. From the available features, the 20 best features were selected for the classification process using the Gaussian Naive Bayes algorithm. Model evaluation was conducted using a confusion matrix with accuracy, precision, recall, and F1-score as evaluation metrics. The test results showed that the Gaussian Naive Bayes model achieved an accuracy of 62.96%, precision of 42.05%, recall of 99.53%, and F1-score of 59.12%. The high recall value indicates that the model was able to identify most of the traffic that constituted DDoS attacks. However, the precision, accuracy, and F1-score values indicate that the model still produced classification errors, particularly in distinguishing between normal traffic and DDoS traffic in a balanced manner. Therefore, the Gaussian Naive Bayes algorithm in this study demonstrated a high capability to identify DDoS attack traffic, as indicated by the recall value of 99.53%, but still had limitations in distinguishing between normal traffic and DDoS traffic in a balanced manner.

Keywords: DDoS, Gaussian Naive Bayes, CICIoT2023, Machine Learning, Intrusion Detectio