

INTISARI

PENGUNAAN ALGORITMA NAÏVE BAYES DENGAN SELEKSI FITUR DAN *FEATURE SCALING* UNTUK MENDETEKSI SERANGAN *DENIAL OF SERVICE*

Havid Sudarsono
18/427579/PA/18539

Serangan *Denial of Service* (DoS) merupakan jenis ancaman siber yang dapat menyebabkan suatu sistem tidak mampu menanggapi permintaan akses dari pengguna yang sah. Penggunaan *Intrusion Detection System* (IDS) menjadi salah satu solusi yang dapat diterapkan untuk mendeteksi adanya serangan DoS. Namun, penerapan IDS juga tidak dapat terlepas dari berbagai tantangan tersendiri seperti tidak adanya jaminan untuk semua jenis serangan dapat terdeteksi. Pendekatan berbasis *machine learning* sudah banyak digunakan di berbagai penelitian untuk mengembangkan sistem pendeteksi intrusi yang lebih baik. Algoritma Naïve Bayes merupakan salah satu algoritma *machine learning* yang sering kali digunakan di dalam sejumlah penelitian untuk mengembangkan model pendeteksi intrusi karena karakteristik algoritma yang sederhana serta memiliki keunggulan pada kecepatan waktu eksekusi. Namun, beberapa penelitian memperoleh bahwa algoritma Naïve Bayes menghasilkan performa yang tidak cukup baik ketika dibandingkan dengan algoritma *machine learning* lainnya.

Pada penelitian ini akan dilakukan pengujian penerapan dua teknik seleksi fitur yang berbeda, yaitu teknik berbasis *Information Gain* dan *Forward Selection*, bersamaan dengan teknik *feature scaling* berupa *MinMax Scaler* pada masing-masing skenario pengujian sebagai cara untuk mengoptimalkan performa algoritma Naïve Bayes yang digunakan untuk mendeteksi serangan *Denial of Service*. Hasil penelitian menunjukkan bahwa model Naïve Bayes memperoleh nilai akurasi yang meningkat sekurang-kurangnya 20% ketika diterapkan teknik seleksi fitur dan teknik *feature scaling* dibandingkan model yang dikembangkan tanpa kedua teknik tersebut. Kemudian, model Naïve Bayes yang dikembangkan dengan menerapkan seleksi fitur *Forward Selection* mampu memperoleh nilai akurasi yang lebih tinggi dibandingkan ketika diterapkan teknik seleksi fitur *Information Gain*, meskipun membutuhkan waktu pelatihan yang lebih lama dengan selisih rata-rata *running time* sebesar 175,93 detik.

Kata kunci: *Denial of Service*, *Intrusion Detection System*, Naïve Bayes

ABSTRACT

THE IMPLEMENTATION OF NAÏVE BAYES ALGORITHM WITH FEATURE SELECTION AND FEATURE SCALING TO DETECT DENIAL OF SERVICE ATTACK

Havid Sudarsono
18/427579/PA/18539

Denial of Service (DoS) attack is a type of cyberthreat which can cause a system to be unable to respond to access requests from legitimate users. The use of an Intrusion Detection System (IDS) is one of the solutions that can be applied to detect DoS attacks. However, the implementation of IDS cannot be separated from its own challenges, such as there is no guarantee that all types of attacks can be detected. Machine learning-based approaches have been widely used in various studies to develop a better intrusion detection system. The Naïve Bayes algorithm is one of the machine learning algorithms that is often used in a number of studies to develop intrusion detection models due to its simple characteristics and the advantage in speed of execution time. However, several studies have found that the Naïve Bayes algorithm did not perform well enough when compared to other machine learning algorithms.

In this study, the use of two different feature selection techniques will be tested, namely Information Gain and Forward Selection based techniques, together with a feature scaling technique in the form of MinMax Scaler in each testing scenario as a way to optimize the performance of the Naïve Bayes algorithm that is used to detect Denial of Service attacks. The result of this study shows that the Naïve Bayes model obtains an increase in accuracy of at least 20% when the feature selection and feature scaling techniques were applied compared to the model which was developed without these two techniques. Then, the Naïve Bayes model which was developed with applying the feature selection technique in the form of Forward Selection can obtain a higher accuracy compared to when the Informatin Gain based feature selection technique was applied, even though it required a longer training time with an average running time difference of 175,93 seconds.

Keywords: Denial of Service, Intrusion Detection System, Naïve Bayes