1. Pendahuluan

Latar Belakang

Di zaman sekarang teknologi di bidang internet berkembang secara pesat. Setiap orang dapat menerima informasi dengan menggunakan atau mengakses internet. Namun internet tidak hanya menyediakan peluang potensial yang positif untuk pengguna saja, di sisi lain internet juga terdapat resiko yang sangat besar yaitu dampak negatif untuk penggunanya. *Denial of Service* (DoS) merupakan serangan yang menyerang di keamanan jaringan komputer. *Denial of Service* (DoS) adalah penolakan layanan dengan memenuhi *traffic* yang menghabiskan *resource* sehingga mengakibatkan pengguna yang lain tidak mendapatkan akses layanan dari komputer yang diserang. Tujuan dari *Denial of Service* (DoS) bukan untuk mencuri informasi dari target, namun tujuan dari penyerang adalah membuat server atau jaringan gagal menyediakan layanan secara normal atau membuat layanannya tidak berguna [1].

Tingginya potensi serangan *Denial of Service* (DoS), maka untuk mengetahui data tersebut merupakan ancaman atau tidak dibutuhkan deteksi akurat terhadap serangan *Denial of Service* (DoS) untuk meningkatkan keamanan jaringan dapat dilakukan dengan pendeteksian intrusi pada jaringan. *Intrusion Detection System* (IDS) adalah suatu system yang mendeteksi dan mengidentifikasi adanya serangan yang terjadi pada suatu jaringan berdasarkan *network-based* dan *host-based* [2].

Intrusion Detection System (IDS) terdapat dua teknik pendekatan dasar untuk mendeteksi serangan yang terjadi pada jaringan, yaitu teknik *Anomaly detection* dan *Signature-based* (dikenal sebagai *Misuse detection*)[3]. Untuk mencari *patters* atau *signatures* dari serangan dikenal. Jika ditemukan cocok maka menghasilkan alarm. *Database Signature* dikenal serangan ditentukan sebuah priori. Di sisi lain, Deteksi anomali [4], mencoba memperkirakan perilaku ‘normal' sistem yang akan dilindungi dan menghasilkan alarm ketika penyimpangan antara perilaku sistem saat ini dan perilaku normal melebihi ambang batas yang telah ditetapkan. Namun metode *Intrusion Detection System* (IDS) yang ada saat ini tidak terlalu akurat[5]. Dan IDS mempunyai kelemahan dalam hasil akurasi yang tidak optimal dan untuk mendeteksi memerlukan waktu *build* model yang lama[11].

Karena dengan metode *Intrusion Detection System* (IDS) tidak terlalu akurat, dalam menyelesaikan masalah di atas akan dipilih metode *machine learning* (ML) yang mendapatkan hasil lebih akurat[5]. Penelitian ini akan menganalisis perbandingan tingkat akurasi antara dua metode *supervised learning* dalam mendeteksi *Denial of Service* (DoS). Dan dengan dua metode *supervised learning* yang berfungsi mengklasifikasi serangan *Denial of Service* (DoS), yaitu *Naïve Bayes* dan PNN. Pada penelitian Vijay D Katkar dan Siddhant Vijay Kulkarni [4] yang menjelaskan tentang performansi metode *Naïve Bayes* dengan teknik *Information Gain* memiliki tingkat akurasi yang cukup tinggi yaitu 98,6%. Namun saat ini tidak ada penelitian tentang analisis perbandingan tingkat akurasi metode Naïve Bayes dan PNN. Oleh karena itu metode yang diusulkan adalah *Naïve Bayes* dan PNN dalam mendeteksi *Denial of Service* (DoS).

Topik dan Batasannya

Berdasarkan latar belakang, rumusan masalah yang diambil adalah bagaimana perbandingan akurasi algoritma *Naïve Bayes* dan PNN dalam memprediksi atau mendeteksi serangan DoS. Adapun batasan masalah yang ada yaitu hanya membandingkan akurasi algoritma *Naïve Bayes* dan PNN serta waktu *build* yang dibutuhkan.

Tujuan

Tujuan penelitian ini untuk menganalisis perbandingan akurasi algoritma *Naïve Bayes* dan PNN dalam mendeteksi serangan DoS serta waktu *build* masing-masing algoritma.

Organisasi Tulisan

Pada Jurnal TA ini dijelaskan hal terkat identifikasi masalah, data yang digunakan, lalu disertakan juga pemodelan dan perancangan sistem yang akan dibangun secara umum untuk menyelesaikan masalah yang dijelaskan pada bagian latar belakang. Pengujian dan hasil analisis dibahas pula dalam jurnal TA ini yang dimana kedua hal tersebut dijadikan rujukan penarikan kesimpulan.