4.2 Analisis Hasil Pengujian

Input layer memiliki 13 neuron karena setiap *record* yang ada di dalam dataset memiliki 13 fitur. *Hidden Layer* memiliki 113.270 neuron, sebanyak *record* yang ada di *data train*. PNN merupakan proses *one feed forward* dan tidak ada *back propagation*. *Summation layer* memiliki 2 neuron yang merepresantikan jumlah kategori pengklasifian dan *output layer* memiliki 1 neuron yang merupakan hasil akhir keputusan. Dapat dilihat pada Tabel 3 algoritma PNN memiliki akurasi tertinggi yaitu 98,06%. Nilai TP (True Positive) merupakan catatan serangan yang dideteksi sebagai serangan, hasil pengujian menghasilkan 5.584 data yang teridentifikasi sebagai TP. Sebanyak 9.567 teridentifikasi sebagai TN (True Negative), TN adalah jumlah catatan normal yang terdeteksi normal. Nilai FP (False Positive) sebanyak 600 yang artinya ada catatan normal yang dideteksi sebagai serangan. Nilai FN (False Negative) adalah jumlah serangan yang sebenarnya namum dideteksi sebagai normal dan di pengujian ini, nilai FN sebanyak 809 data. Algoritma PNN menghasilkan nilai akurasi yang lebih baik daripada yang lain karena perhitungan PNN sangat detail dan berbeda daripada algortima yang lain, terlihat pada semua neuron yang ada di *input layer* dihitung dengan model Gaussian terhadap semua neuron yang ada di *data train*. Hal tersebut dapat membantu meminimalisir kesalahan dalam proses pengklasifikasian. Model Gaussian juga sangat mendukung algoritma PNN ini, karena terbukti saat dibandingkan dengan SGD, nilai akurasi Gaussian jauh lebih baik. Perhitungan Gaussian bergantung pada nilai standar deviasi telah ditentukan berdasarkan hasil beberapa ekperimen, pada penelitian ini nilai std=0,001. Nilai ini sangat berpengaruh karena mempengaruhi pesebaran data. Fungsi Gaussian dengan distribusi normal dinilai lebih optimal dibandingkan SGD.

Nilai akurasi PNN merupakan nilai yang tertinggi daripada algortima lainnya dan PNN memiliki kelebihan yang tidak dimiliki oleh algortima lain. Kelebihan PNN [10] adalah stuktur paralel yang inheren (berhubungan erat), dapat dilihat dalam proses algoritma PNN dimana semua atribut data input akan dihitung secara matematis dengan seluruh atribut yang ada di data train sehingga dapat dipastikan bahwa record data test akan diuji serinci mungkin pada data train untuk meminimalisir kesalahan dalam proses pengklasifikasian. PNN juga menjamin menjadi *classifer* yang optimal karena ukuran data train yang terus meningkat. Sampel training pada PNN dapat ditambahkan atau dihapus tanpa pelatihan ulang yang intensif.

5. Kesimpulan

Jaringan komputer saat ini harus diamankan dari serangan-serangan yang semakin canggih. *Intrusion Detection System* (IDS) memegang peranan penting dalam menyelesaikan masalah keamanan jaringan komputer. Penelitian ini membuktikan bahwa *machine learning* dapat meningkatkan performansi IDS jika dibandingkan dengan metode tradisional. Beberapa model algoritma telah diuji untuk menentukan akurasi yang terbaik. Dan nilai akurasi yang paling unggul adalah algoritma *Probabilistic Neural Network* (PNN) yaitu 98,06%. Sehingga dapat disimpulkan bahwa PNN lebih baik dalam mengatasi masalah keamanan jaringan komputer dan dapat meningkatkan keamanan jaringan komputer.

Saran untuk penelitian selanjutnya adalah melakukan eksperimen terhadap data *real traffic* untuk mengevaluasi kembali apakah algoritma PNN sesuai dengan *environment* sistem jaringan komputer tersebut.

Daftar Pustaka

[1] A review of machine learning techniques efficiency in dos attack detection. *International Journal of Scientific Research*, 6:461–462, 2017.

[2] S. K. Biswa. Intrusion detection using machine learning: A comparison study. *International Journal of Pure and Applied Mathematics*, 119:101–114, 2018.

[3] S. Devaraju and D. S. Ramakrishnan. Performance analysis of intrusion detection system using various neural network classifier. *International Conference on Recent Trends in Information Technology (ICRTIT)*, pages 1033–1038, 2011.

[4] L. Dhanabal and P. Shantharajah. A study on nsl-kdd dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced in Computer and Communication Engineering*, 4:446–452, 2015.

[5] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36:16–24, 2013.

[6] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne. Evaluating computer intrusion detection systems: A survey of common practices. *ACM Computing Surveys*, 48:12:1–12:41, 2015.

[7] L. Ning. Network intrusion classification based on probabilistic neural network. *International Conference on Computational and Information Sciences*, pages 57–59, 2013.

[8] O. Osanaiye, H. Cai, K.-K. R. Choo, A. Dehghantanha, Z. Xu, , and M. Dlodlo. Ensemble-based multi-filter feature selection method for ddos detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, pages 1–10, 2016.

[9] C. E. Rasmussen and C. K. I. Williams. Gaussian processes for machine learning. *The MIT Press*, pages 1–266, 2006.

[10] S. S. Sawant and P. S. Topannavar. Introduction to probabilistic neural network. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5:279–283, 2015.

[11] D. School. Simple guide to confusion matrix terminology. `http://www.dataschool.io/simple-guide-to-confusion-matrix-terminology/`, 2008. Online; Accessed 5 April 2019.

[12] M. Zamani. Machine learning techniques for intrusion detection. *arXiv Computer Science*, pages 1–10, 2013.

[13] M. Zhang, J. Guo, B. Xu, and J. Gong. Detecting network intrusion using probabilistic neural network. *11th International Conference on Natural Computation (ICNC)*, pages 1151–1158, 2016.