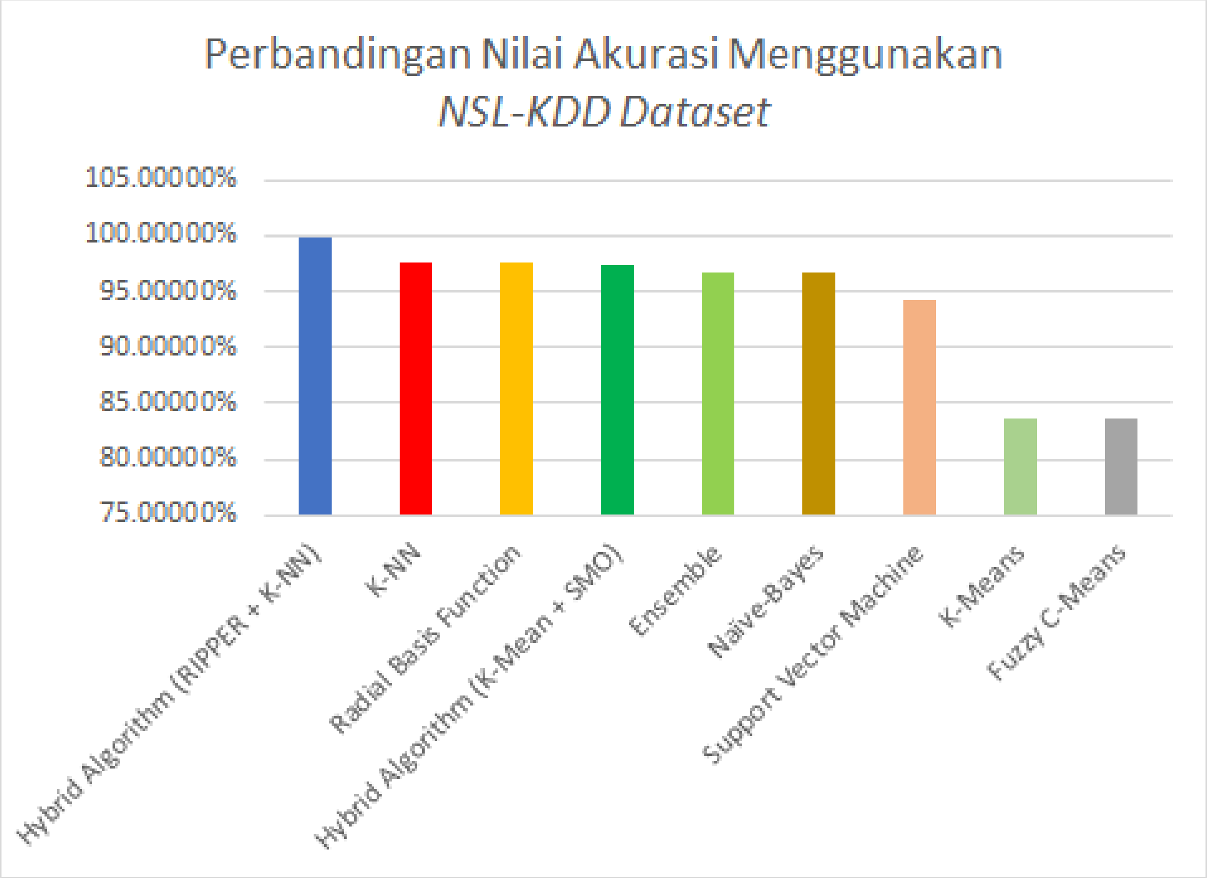
4.3 Perbandingan Nilai Akurasi dengan Penelitian Lainnya Menggunakan *NSL-KDD Dataset*



Gambar 6. Perbandingan Nilai Akurasi

5. Kesimpulan

Penggunaan dua algoritma yang berbeda karakteristik, yaitu algoritma RIPPER dan algoritma *K-Nearest Neighbour* (K-NN) mampu membangun *model detection* yang bisa menghasilkan akurasi yang akurat baik untuk data dengan jenis anomali yang sudah dipelajari maupun yang belum pernah dipelajari. Hasil akurasi terbaik untuk seluruh pengujian yang dihasilkan akurasi terbaik sebesar 99.89522%. Penggunaan nilai k yang menghasilkan akurasi terbaik adalah menggunakan nilai k=1. Untuk penelitian selanjutnya coba dilakukan proses deteksi anomali terhadap data trafik jaringan secara *realtime*.

Daftar Pustaka

[1] M. Ahmed, A. Naser Mahmood, and J. Hu. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 2016.

[2] K. J. P. D. Barford, P. and A. Ron. A signal analysis of network traffic anomalies. *In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment*, 2002.

[3] P. Barford and D. Plonka. Characteristics of network traffic flow anomalies. *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, 2001.

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita. Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys Tutorials*, 2014.

[5] H. Bostani and M. Sheikhan. Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach. *Computer Communications*, 2017.

[6] J. A. Bul'ajoul, W. and M. Pannu. Improving network intrusion detection system performance through quality of service configuration and parallel technology. *Journal of Computer and System Sciences*, 2015.

[7] M. S. D. Butun, I. and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys Tutorials*, 2014.

[8] B. A. Chandola, V. and V. Kumar. Anomaly detection: A survey. *ACM Computing Surveys*, 2009.

[9] R. J. J. P. C. de Assis, M. V. O. and M. L. Proença. A seven-dimensional flow analysis to help autonomous network management. *Information Sciences*, 2014.

[10] D. M. Debar, H. and A. Wespi. Towards a taxonomy of intrusion–detection systems. *Computer Networks*, 1999.

[11] L. Dhanabal and D. S. Shantharajah. A study on nsl-kdd dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 2015.

[12] H. P. K. B. Duffield, N. and H. Ringberg. Rule-based anomaly detection on ip flows. *In IEEE INFOCOM 2009—28th Conference on Computer Communications*, 2009.

[13] R. Fontugne and K. Fukuda. A hough-transform-based anomaly detector with an adaptive time interval. *ACM SIGAPP Applied Computing Review*, 2011.

[14] S. M. A. M. Gadal and R. A. Mokhtar. Anomaly detection approach using hybrid algorithm of data mining technique. *International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE)*, 2017.

[15] L. W. Ghorbani, A. A. and M. Tavallaee. Network attacks. *Advances in Information Security*, 2010.

[16] R. J. J. P. C. C. L. F. A.-M. J. F. Jr., Gilberto Fernandes and M. L. P. Jr. A comprehensive survey on network anomaly detection. *Telecommunication Systems*, 2019.

[17] K. B. Jung, J. and M. Rabinovich. Flash crowds and denial of service attacks. *In Proceedings of The 11th International Conference on World Wide Web*, 2002.

[18] R. A. Kemmerer and G. Vigna. Intrusion detection: A brief history and overview. *Computer*, 2002.

[19] W. Lee and S. Stolfo. Datamining approaches for intrusion detection. *In Proceedings of 7th USENIX security symposium, USENIX Association*, 1998.

[20] A. Lof and R. Nelson. Annotating network trace data for anomaly detection research. *In 2014 IEEE 39th conference on local computer networks workshops (LCN workshops)*, 2014.

[21] S.-F. A. Marnerides, A. K. and A. Mauthe. Traffic anomaly diagnosis in internet backbone networks: A survey. *Computer Networks*, 2014.

[22] R. A. Maxion and T. N. Townsend. Masquerade detection using truncated command lines. *In International conference on dependable systems and networks*, 2002.

[23] L. Meng Hui and A. Jones. Network anomaly detection system: The state of art of network behaviour analysis. *In International conference on convergence and hybrid information technology 2008*, 2008.

[24] V. M.-K. S. A. A. Milenkoski, A. and B. D. Payne. Evaluating computer intrusion detection systems: A survey of common practices. *ACM Computing Surveys*, 2015.

[25] M. M. M. Mouton, F. and H. S. Venter. Social engineering from a normative ethics perspective. *In Information security for South Africa*, 2013.

[26] H. H. Pan, J. and Y. Liu. Human behavior during flash crowd in web surfing. physica a: Statistical mechanics and its applications. *Elsevier*, 2014.

[27] A. Patcha and J. M. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 2007.

[28] K. H. Purwanto, Yudha and B. Rahardjo. Traffic anomaly detection in ddos flooding. *International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2014.

[29] D. D. Saputro, I. N. Yulita, and Shaufiah. *Analisis dan Implementasi Algoritma Hybrid (Eager Learning dan Lazy Learning) Pada Intrusion Detection System*. Universitas Telkom, 2012.

[30] A. K. Shrivas and A. K. Dewangan. An ensemble model for classification of attacks with feature selection basedon kdd99 and nsl-kdd data set. *International Journal of Computer Applications*, 2014.

[31] T. S. Sobh. Wired andwireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards Interfaces*, 2006.

[32] B. S. Stakhanova, N. and J. Wong. On the symbiosis of specification-based and anomaly-based detection. *Computers Security*, 2010.

[33] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani. A detailed analysis of the kdd cup 99 data set. *Computational Intelligence In Security and Defense Aplication (CISDA)*, 2009.

[34] M. Thottan and C. Ji. Anomaly detection in ip networks. *IEEE Transactions on Signal Processing*, 2003.

[35] M. W. J. C. Xiuyao, S. and S. Ranka. Conditional anomaly detection. *IEEE Transactions on Knowledge and Data Engineering*, 2007.