DAFTAR PUSTAKA

[1] R. T. Watson, *Information Systems*. Global Text Project, 2007.

[2] I. S. A. and C. A. ISACA, "Cybersecurity Fundamentals Glossary," 2016.

[3] B. Rahardjo, *Keamanan Sistem Informasi Berbasis Internet*, Versi 5.1., vol. 0. PT. Insan Infonesia - Bandung & PT. Indocisc - jakarta, 2002.

[4] R. Bace and P. Mell, "Intrusion Detection System," *NIST Spec. Publ. Intrusion Detect. Syst.*, pp. 1–51, 2001.

[5] Symantec Corporation, "Internet Security Threat Report 2015 Appendices," 2015.

[6] Cisco, "Cisco 2017 Annual Cybersecurity Report," 2017.

[7] H. M. Imran, A. Bin Abdullah, M. Hussain, and S. Palaniappan, "Intrusions Detection based on Optimum Features Subset and Efficient Dataset Selection," *IJEIT*, vol. 2, no. 6, pp. 265–270, 2012.

[8] Federal Office for Information Security (BSI), "Industrial Control System Security Top 10 Threats and Countermeasures 2016," 2016.

[9] E. Bloedorn, A. Christiansen, and W. Hill, "Data mining for network intrusion detection: How to get started," *Discovery*, 2001.

[10] H.-J. Liao, C.-H. R. Lin, and Y.-C. Lin, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2012.

[11] Q. Yang, X. Wu, P. Domingos, C. Elkan, J. Gehrke, J. Han, D. Heckerman, D. Keim, J. Liu, D. Madigan, G. Piatetsky-Shapiro, V. V Raghavan, R. Rastogi, S. J. Stolfo, A. Tuzhilin, and B. W. Wah, "10 Challenging Problems in Data Mining Research," *Int. J. Inf. Technol. Decis. Mak.*, vol. 5, no. 4, pp. 597–604, 2006.

[12] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2014*, 2009.

[13] S. Kumar Shrivastava and P. Jain, "Effective Anomaly based Intrusion Detection using Rough Set Theory and Support Vector Machine," *Int. J. Comput. Appl.*, vol. 18, no. 3, pp. 35–41, 2011.

[14] P. N. S. Chandolikar and P. (Dr. . V.D. Nandavadekar, "Selection of Relevant Feature for Intrusion Attack Classification by Analyzing KDD Cup 99," *MIT Int. J. Comput. Sci. Inf. Technol.*, vol. 2, no. 2, pp. 85–90, 2012.

[15] A. Jacobus and E. Winarko, "Penerapan Metode Support Vector Machine pada Sistem Deteksi Intrusi secara Real-time," *Ijccs*, vol. 8, no. 1, pp. 13–24, 2014.

[16] D. A. Antony, G. Singh, and E. J. Leavline, "Data Mining in Network Security - Techniques & Tools : a Research Perspective," *J. Theor. Appl. Inf. Technol.*, vol. 57, no. 2, pp. 269–278, 2013.

[17] R.-C. Chen, K.-F. Cheng, and C.-F. Hsieh, "Using Rough Set and Support Vector Machine for Network Intrusion Detection," *Netw. Secur.*, vol. 1, p. 13, 2010.

[18] I. Singh Arora, G. Kaur Bhatia, and A. Professor, "Comparative Analysis of Classification Algorithms on KDD " 99 Data Set," *I.J. Comput. Netw. Inf. Secur.*, vol. 9, no. 9, pp. 34–40, 2016.

[19] W. Lee and S. J. Stolfo, "A framework for constructing features and models for intrusion detection systems," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp. 227–261, Nov. 2000.

[20] B. A. Pratomo and R. M. Ijtihadie, "Sistem Deteksi Intrusi Menggunakan N-Gram Dan Cosine Similarity," *JUTI J. Ilm. Teknol. Inf.*, vol. 14, no. 1, p. 108, 2016.

[21] S. Peddabachigari, A. Abraham, and J. Thomas, "Intrusion detection systems using decision trees and support vector machines," *Int. J. Appl. Sci. Comput.*, pp. 118–134, 2004.

[22] S. Benferhat, K. Sedki, and K. Tabia, "Preprocessing Rough Network Traffic for Intrusion Detection Purposes," in *IADIS International Telecommunications, Networks and Systems*, 2007, pp. 105–109.

[23] J. W. de Godoy and Lee Luan Ling, "Network Traffic Monitoring and Analysis," in *The State of the Art in Intrusion Prevention and Detection*, 1st ed., A.-S. K. Pathan, Ed. CRC Press, 2014, pp. 23–44.

[24] O. Maimon and L. Rokach, *Data Mining and Knowledge Discovery Handbook*, 2nd ed. Springer, 2010.

[25] I. Pramudiono, "Pengantar Data Mining : Menambang Permata Pengetahuan di Gunung Data," *Kuliah Umum Ilmu Komputer.com*, pp. 1–4, 2003.

[26] H. Zhang, L. Jiang, and J. Su, "Augmenting Naive Bayes for Ranking," in *ICML '05 Proceedings of the 22nd international conference on Machine learning*, 2005, vol. 1, pp. 1020–1027.

[27] L. Vinet and A. Zhedanov, "A 'missing' family of classical orthogonal polynomials," *CRC*, pp. 29–54, Nov. 2010.

[28] H. Han, W.-Y. Wang, and B.-H. Mao, "Borderline-SMOTE: A New Over-Sampling Method in Imbalanced Data Sets Learning," *Adv. Intell. Comput.*, vol. 17, no. 12, pp. 878–887, 2005.

[29] E. Alpaydin, *Introduction to Machine Learning*, Third edit. The MIT Press Cambridge, Massachusetts London, England, 2014.

[30] M. M. Jain and P. V. Richariya, "An Improved Techniques Based on Naive

Bayesian for Attack Detection," *Int. J. Emerg. Technol. Adv. Eng. Website www.ijetae.com*, vol. 2, no. 1, pp. 324–331, 2012.

[31] X. Wu and V. Kumar, *The Top Ten Algorithms in Data Mining*. CRC Press, 2009.

[32] D. K. Bhattacharyya and J. K. Kalita, *Network Anomaly Detection A Machine Learning Perspective*. CRC Press, 2014.

[33] D. K. Ahirwar, S. K. Saxena, and M. S. Sisodia, "Anomaly Detection by Naive Bayes & RBF Network," *Int. J. Adv. Res. Comput. Sci. Electron. Eng.*, vol. 1, no. 1, pp. 14–18, 2012.

[34] A. Valdes and K. Skinner, "Adaptive, Model-Based Monitoring for Cyber Attack Detection," in *Recent Advances in Intrusion Detection*, 2000, pp. 80–93.

[35] L. Koc, T. A. Mazzuchi, and S. Sarkani, "A network intrusion detection system based on a Hidden Naive Bayes multiclass classifier," *Expert Syst. Appl.*, vol. 39, no. 18, pp. 13492–13500, 2012.

[36] J. Han, M. Kamber, and J. Pei, *Data Mining : Concepts and Techniques Third Edition*. Elsevier, Morgan Kaufmann Publisher, 2011.

[37] I. H. Witten, E. Frank, and M. a. Hall, *Data Mining Practical Machine Learning Tools and Techniques Third Edition*, vol. 277. 2011.

[38] J. Yao, S. Zhao, and L. Fan, "An Enhanced Support Vector Machine Model for Intrusion Detection," *Rough Sets Knowl. Technol.*, pp. 538–543, 2006.

[39] S. A. Mulay, P. R. Devale, and G. V. Garje, "Intrusion Detection System Using Support Vector Machine and Decision Tree," *Int. J. Comput. Appl.*, vol. 3, no. 3, pp. 40–43, 2010.

[40] Y. B. Bhavsar and K. C. Waghmare, "Intrusion Detection System Using Data Mining Technique : Support Vector Machine," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 3, 2013.

[41] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001.

[42] "KDD Cup 1999 Data." [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed: 01-Jan-2017].

[43] F. Gharibian and A. A. Ghorbani, "Comparative Study of Supervised Machine Learning Techniques for Intrusion Detection," *Fifth Annu. Conf. Commun. Networks Serv. Res.*, vol. 14, no. 3, pp. 5–10, 2007.

[44] J. Zhang and M. Zulkernine, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection," *2006 IEEE Int. Conf. Commun.*, vol. 5, no. c, pp. 2388–2393, 2006.

[45] G. P. Dubey, P. N. Gupta, and R. K. Bhujade, "A Novel Approach to Intrusion Detection System using Rough Set Theory and Incremental

SVM," *Soft Comput.*, no. 1, pp. 14–18, 2011.

[46] A. S. O. and D. O. A. Adetunmbi A.Olusola., "Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features," *World Congr. Eng. Comput. Sci.*, vol. Vol I, no. October 20-22, 2010, 2010.

[47] H. Jiawei, M. Kamber, J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, Third. Elsevier, 2012.

[48] S. S. Sivatha Sindhu, S. Geetha, and A. Kannan, "Decision Tree Based Light Weight Intrusion Detection using a Wrapper Approach," *Expert Syst. with Appl. Elsevier*, vol. 39, no. 1, pp. 129–141, 2012.

[49] H. G. Kayacık, A. N. Zincir-heywood, and M. I. Heywood, "Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets," in *Proceedings of the Third Annual Conference on Privacy, Security and Trust. Kessel,* 2005, pp. 3–8.

[50] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2670–2679, 2015.

[51] M. Aggarwal and Amrita., "Performance Analysis Of Different Feature Selection Methods In Intrusion Detection," *Int. J. Sci. Technol. Res.*, vol. 2, no. 6, pp. 225–231, 2013.

[52] R. R. Bouckaert, E. Frank, M. Hall, R. Kirkby, P. Reutemann, A. Seewald, and D. Scuse, "WEKA Manual for Version 3-6-3," *University of Waikato*. 2010.

[53] Y. Wahba, E. ElSalamouny, and G. ElTaweel, "Improving the Performance of Multi-class Intrusion Detection Systems using Feature Reduction," *IJCSI*, vol. 12, no. 3, pp. 255–262, 2015.

[54] S. Paliwal, "Denial-of-Service , Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm," *Int. J. Comput. Appl.*, vol. 60, no. 19, pp. 57–62, 2012.

[55] J. I. Maletic and A. Marcus, *Data Mining and Knowledge Discovery Handbook*, 2nd ed. Springer, 2010.

[56] Tim, "machine learning - How to interpret error measures in Weka output- Cross Validated," 2015. [Online]. Available: https://stats.stackexchange.com/questions/131267/how-to-interpret-error-measures-in-weka-output. [Accessed: 16-Jun-2017].

[57] MathsIsFun.com, "Correlation," 2016. [Online]. Available: http://www.mathsisfun.com/data/correlation.html. [Accessed: 25-Apr-2017].

.