IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

Evaluation of Efficient Classification Algorithm for Intrusion Detection System

V. Priyalakshmi[1] and Dr. R. Devi[2]
Assistant Professor, Department of Computer Science[1]
SRM Arts & Science College, Chennai, Tamil Nadu, India[1]
Associate Professor, Department of Computer Science[2]
Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India[2]
kumaran.durairaj.kd@gmail.com[1] and devi.scs@velsuniv.ac.in[2]

Abstract: *Intrusion detection system is one of the most significant network security problems in the technology world. To improve the Intrusion Detection System (IDS) many machine learning methods are implemented. In order to develop the performance of IDS, different classification algorithms are applied to detect different types of attacks. For building efficient IDS is not an easy task and choosing a suitable classification algorithm. The best method is to test the Performance of the different classification algorithms and select best method from them. This paper aim is to assemble an IDS model in terms of confusion matrix, accuracy, recall, precision, f-score, specificity and sensitivity. It also provides a detailed comparison with the dataset, data preprocessing, number of features selected, feature selection technique, classification algorithms, and evaluation performance of algorithms described in the intrusion detection system.*

Keywords: IDS, NSL-KDD, SVM, Confusion Matrix, Feature Selection, Classification Algorithm

REFERENCES

[1]. Bace, R. (1998). An Introduction to Intrusion Detection & Assessment. Infidel, Inc. for ICSA, Inc
[2]. Karthikeyan, K. R. & Indra, A. (2010). Intrusion Detection Tools and Techniques a Survey.International Journal of Computer Theory and Engineering, 2(6): 1793-8201
[3]. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques,datasets and challenges. Cybersecurity 2019, 2, 20.
[4]. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J.; Alazab, A. A Novel Ensemble of Hybrid IntrusionDetection System for Detecting Internet of Things Attacks. Electronics 2019, 8, 1210.
[5]. Alazab, A.; Hobbs, M.; Abawajy, J.; Khraisat, A.; Alazab, M. Using response action with intelligent intrusiondetection and prevention system against web application malware. Inf. Manag. Comput. Secur. 2014, 22,431–449.
[6]. Alazab, A.; Hobbs, M.; Abawajy, J.; Alazab, M. Using feature selection for intrusion detection system.In Proceedings of the 2012 International Symposium on Communications and Information Technologies(ISCIT), Gold Cost, Australia, 2–5 October 2012; pp. 296–301.
[7]. Alazab, A.; Abawajy, J.; Hobbs, M.; Khraisat, A. Crime toolkits: The current threats to web applications. J. Inf.Priv. Secur. 2013, 9, 21–39
[8]. Saranyaa, T.,Sridevib, S.,Deisyc, C., Tran Duc Chungd, Ahamed Khane, M. K. A. (2020).Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review.Third International Conference on Computing and Network Communications (CoCoNet'19),Procedia Computer Science 171 (2020) 1251–1260.
[9]. Nguyen, H. A. and Choi, D. (2008). Application of data mining to network intrusion detection: classifier selection model.Asia-Pacific Network Operations and Management Symposium. Springer, 2008, pp. 399–408.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

[10]. Lahre, M. K., Dhar, M. T.,Suresh, D., Kashyap, K. and Agrawal, P. (2013). Analyze different approaches for ids using kdd 99 data set," International Journal on Recent and Innovation Trends in Computing and Communication, 1(8): 645–651.

[11]. Haddadi, F.,Khanchi, S., Shetabi, M. and Derhami, V. (2010). Intrusion detection and attack classification using feed-forward neural network.Computer and Network Technology (ICCNT), 2010 Second International Conference on. IEEE, 2010, pp. 262–266.

[12]. Alsharafat, W. (2013). Applying artificial neural network and extended classifier system for network intrusion detection. International Arab Journal of Information Technology (IAJIT), vol. 10, no. 3, 2013.

[13]. Bhargava, N., Sharma, G., Bhargava, R. and Mathuria, M. (2013). Decision tree analysis on j48 algorithm for data mining, Proceedings of International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, 2013.

[14]. C. Fleizach and S. Fukushima, "A naive bayes classifier on 1998 kdd cup," 1998.

[15]. Alkasassbeh,M.,Al-Naymat, G.,Hassanat, A. B. and Almseidin, M. (2019). Detecting distributed denial of service attacks using data mining techniques, International Journal of Advanced Computer Science & Applications, 1(7): 436–445.

[16]. Mulay, Snehal&Devale, P.R. &Garje, Goraksh. (2010). Intrusion Detection System Using Support Vector Machine and Decision Tree. International Journal of Computer Applications. 3. 10.5120/758-993.

[17]. Khan, Latifur&Awad, M. &Thuraisingham, Bhavani. (2007). A new intrusion detection system using support vector machines and hierarchical clustering. VLDB Journal. 16. 507-521. 10.1007/s00778-006-0002-5.

[18]. AnsamKhraisat, Iqbal Gondal, Peter Vamplew, JoarderKamruzzaman and Ammar Alazab (2020). Hybrid Intrusion Detection System Based on theStacking Ensemble of C5 Decision Tree Classifier andOne Class Support Vector Machine. Electronics. 2020, 9, 173; doi:10.3390/electronics9010173, www.mdpi.com/journal/

[19]. Othman, S.M., Ba-Alwi, F.M., Alsohybe, N.T. et al. Intrusion detection model using machine learning algorithm on Big Data environment. J Big Data5, 34 (2018). https://doi.org/10.1186/s40537-018-0145-4

[20]. Mohamed El Boujnouni and Mohamed Jedra (2018).New Intrusion Detection System Based onSupport Vector Domain Description withInformation Gain Metric" International Journal of Network Security, 20(1): 25 – 34.

[21]. Vipin, Das & Vijaya, Pathak &Sattvik, Sharma &Sreevathsan, & Srikanth M. V. N. N. S., &Gireesh. T. (2010). Network Intrusion Detection System Based On Machine Learning Algorithms. International Journal of Computer Science & Information Technology. 2. 10.5121/ijcsit.2010.2613

[22]. Samra Zafar, Muhammad Kamran, Xiaopeng Hu (2019). Intrusion-Miner: A Hybrid Classifier for IntrusionDetection using Data Mining. International Journal of Advanced Computer Science and Applications, Vol. 10, No. 4, 2019.

[23]. Chung, Yuk & Wahid, Noorhaniza. (2012). A hybrid network intrusion detection system using simplified swarm optimization (SSO). Applied Soft Computing. 12. 3014–3022. 10.1016/j.asoc.2012.04.020.

[24]. Almseidin, M., Alzubi, M., Kovacs, S. and Alkasassbeh, M. (2017). Evaluation of machine learning algorithms for intrusion detection system, 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 2017, pp. 000277-000282, doi: 10.1109/SISY.2017.8080566.

[25]. Jayshree Jha and Leena Ragha (2013). Intrusion Detection System using Support Vector Machine. IJAIS Proceedings on International Conference and workshop on Advanced Computing 2013 ICWAC(3):25-30, June 2013

[26]. Enache, A. and Patriciu, V. V. (2014).Intrusion's detection based on Support Vector Machine optimized with swarm intelligence. 2014 IEEE 9th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2014, pp. 153-158, doi: 10.1109/SACI.2014.6840052.

[27]. Manickam, M., Rajagopalan, S.P. A hybrid multi-layer intrusion detection system in cloud. Cluster Comput22, 3961–3969 (2019). https://doi.org/10.1007/s10586-018-2557-5

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

[28]. Goel, L. (2020). An extensive review of computational intelligence-based optimization algorithms: trends and applications. Soft Computing.24,16519–16549 (2020). https://doi.org/10.1007/s00500-020-04958-w

[29]. P. Amudha,1 S. Karthik,2 and S. Sivakumari, "A Hybrid Swarm Intelligence Algorithm for Intrusion DetectionUsing Significant Features", Hindawi Publishing Corporation Scientific World Journal Volume 2015, Article ID 574589, 15 pagehttp://dx.doi.org/10.1155/2015/574589.

[30]. Adeel Hashmi and Tanvir Ahmad , "FAAD: A Self-Optimizing Algorithm for Anomaly Detection", The International Arab Journal of Information Technology, Vol. 17, No. 2, March 2020

[31]. Thiruvenkadam, Kalaiselvi& Perumal, Nagaraja& Z, Abdul. (2017). A Review on Glowworm Swarm Optimization. International Journal of Information Technology. 3. 49-56.

[32]. Kaipa, Krishnanand& Ghose, Debasish. (2009). Glowworm Swarm Optimization: A New Method for Optimising Multi-Modal Functions. International Journal of Computational Intelligence Studies. 1. 10.1504/IJCISTUDIES.2009.515637.

[33]. Kumar, A. S. A., Arpitha, K., Latha, M. N. and Sahana, M. (2017). A novel approach for intrusion detection system using feature selection algorithm. International Journal of Computational Intelligence Research. 13(8): 1963 – 1976.

[34]. Kuang, F., Xu, W.& Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusiondetection. Applied Soft Computing Journal, 18, 178–184, 2014.

[35]. Wathiq, L. A.,Zulaiha, A. O. &Mohd. Z. A (2017). Multi-Level Hybrid Support Vector Machine andExtreme Learning Machine based on Modified K-means for Intrusion Detection System, ExpertSystems with Applications, 67, 296-303, 2017.