















## REFERENCES

- [1] W. Noonan, I. Dubrawsky, "Firewall fundamentals", Pearson Education, 2006.
- [2] Q. A. Al-Haija, S. Zein-Sabatto, "An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks" *Electronics*, MDPI, vol. 9, no. 12: paper no. 2152., 2020.
- [3] E. Ucar, E. Ozhan, "The Analysis of Firewall Policy Through Machine Learning and Data Mining", *Wireless Personal Communication*, Springer, vol. 96, p.p. 2891–2909, 2017.
- [4] G. Caspi, "Introducing Deep Learning: Boosting Cybersecurity with an Artificial Brain. Informa Tech" Dark Reading, *Analytics* <http://www.darkreading.com/analytics>, 2016.
- [5] Q.A. Al-Haija, C.D. McCurry, S. Zein-Sabatto, "Intelligent Self-reliant Cyber-Attacks Detection and Classification System for IoT Communication Using Deep Convolutional Neural Network", Selected Papers from 12<sup>th</sup> International Networking Conference. INC 2020. *Lecture Notes in Networks and Systems*, vol.180. Springer, 2021.
- [6] J. Brownlee, "4 Types of Classification Tasks in Machine Learning", Python Machine Learning, Machine Learning Mastery, 2020.
- [7] S. Haykin, "Neural Networks and Learning Machines. 3<sup>rd</sup> Edition, Pearson publications, ISBN-13: 978-0-13-147139-9, 2009.
- [8] C. C. Aggarwal, "Machine Learning with Shallow Neural Networks", Neural Networks and Deep Learning. Springer, 2019.
- [9] Fei-Fei. CS231n: Convolutional Neural Networks for Visual Recognition. Computer Science, Stanford University. Available online: <http://cs231n.stanford.edu>, 2019.
- [10] J. S. Meneses, Z.R. Chavez, J.G. Rodriguez, "Compressed kNN: K-Nearest Neighbors with Data Compression" *Entropy*, MDPI, vol. 21, no. 3, paper no. 234, 2019.
- [11] Y.Y. Song, Y. Lu, "Decision tree methods: applications for classification and prediction. Shanghai Arch Psychiatry", *PMID: 26120265; PMCID: PMC4466856*, vol. 27, no.2, p.p.130-5, 2015.
- [12] B. A. Tama, K. H. Rhee, "An extensive empirical evaluation of classifier ensembles for intrusion detection task", *International Journal Computer Systems Science and Engineering*, CRL Publishing Ltd, vol. 32, no.2, p.p.149-158, 2017.
- [13] A. Ghose, "Support Vector Machine (SVM) Tutorial: Learning SVMs from examples". Medium: towards data science, 2017.
- [14] R. Garg, "Types of Classification Algorithms", Analytics India Magazine, 2018.
- [15] F. Ertam, M. Kaya, "Classification of firewall log files with multi-class support vector machine," in *Proc. Of 6<sup>th</sup> International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, pp. 1-4, 2019.
- [16] Q. A. Al-Haija, L. Tawalbeh, "Autoregressive Modeling and Prediction of Annual Worldwide Cybercrimes for Cloud Environments," in *Proc. Of 10<sup>th</sup> International Conference on Information and Communication Systems (ICICS)*, 2019, pp. 47-51.
- [17] D. Appelt, C. D. Nguyen, A. Panichella, L. C. Briand, "A Machine-Learning-Driven Evolutionary Approach for Testing Web Application Firewalls," *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 733-757, 2018, doi: 10.1109/TR.2018.2805763.
- [18] E. Ucar, E. Ozhan, "The Analysis of Firewall Policy Through Machine Learning and Data Mining", *Wireless Personal Communication*, Springer, vol. 96, p.p. 2891–2909, 2017.
- [19] A. M. Vartouni, M. Teshnehlab, S. S. Kashi, "Leveraging deep neural networks for anomaly-based web application firewall", *IET Information Security*, vol. 13, p.p. 352-361, 2019.
- [20] F. Ertam, "An efficient hybrid deep learning approach for internet security", *Physica A: Statistical Mechanics and its Applications*, Elsevier, vol. 535, 2019
- [21] J.J. Praise, R.J Raj, J.V. Benifa, "Development of Reinforcement Learning and Pattern Matching (RLPM) Based Firewall for Secured Cloud Infrastructure", *Wireless Personal Communication*, Springer, vol.115, p.p. 993–1018, 2020.
- [22] G. Bendiab, S. Shiaeles, A. Alruban, N. Kolokotronis, "IoT Malware Network Traffic Classification using Visual Representation and Deep Learning", in *Proc. Of 6<sup>th</sup> IEEE Conference on Network Softwarization (NetSoft)*, Ghent, Belgium, 29 June–3 July 2020; pp. 444–449.
- [23] R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, N. Kolokotronis, "Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualization", in *Proc. Of Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lecture Notes in Computer Science*; Springer, vol.11660, 2019
- [24] I. Baptista, S. Shiaeles, N. Kolokotronis, "A Novel Malware Detection System Based On Machine Learning and Binary Visualization", in *Proc. Of IEEE International Conference on Communications (IEEE ICC)*, China, pp. 1–6, 2019.
- [25] K.A. Taher, B.M. Jisan, M.M Rahman, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection", in *Proc. Of International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, South Asia, 10–12 January 2019; pp. 643–646.
- [26] X. Gao, C. Shan, C. Hu, Z. Niu, Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection", *IEEE Access*, vol. 7, p.p. 82512–82521, 2019.
- [27] Q. A. Al-Haija, M. Alkhatib, A. B. Jaafar, "Choices on Designing Gf(P) Elliptic Curve Coprocessor Benefiting from Mapping Homogeneous Curves in Parallel Multiplications", *International Journal on Computer Science and Engineering (IJCSE)*, ISSN: 0975-3397, vol. 3 no. 2, 2011.
- [28] S. Sapre, P. Ahmadi, K. Islam, "A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets through Various Machine Learning Algorithms", *arXiv:1912.13204v1*, 2019.
- [29] M.M. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, J. Li, "A few-shot deep learning approach for improved intrusion detection", 2017 in *Proc. Of IEEE 8<sup>th</sup> Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, NY, USA, 19–21 October 2017; pp. 456–462.
- [30] A. Javaid, Q. Niyaz, W. Sun, M. Alam, "A Deep Learning Approach for Network Intrusion Detection System", in *Proc. Of 9<sup>th</sup> EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, NY, USA, 24 May 2016; pp. 21–26.
- [31] Y. Imamverdiyev, L. Sukhostat, "Anomaly detection in network traffic using extreme learning machine", in *Proc. Of IEEE 10<sup>th</sup> International Conference on Application of Information and Communication Technologies (AICT)*, Azerbaijan, 12–14 October 2016; pp. 1–4.
- [32] UCI: Machine Learning Repository, "Internet Firewall Data Set", Center for Machine Learning and Intelligent Systems, 2019.
- [33] A. Wang, "Encode Smarter: How to Easily Integrate Categorical Encoding into Your Machine Learning Pipeline", Feature Labs. <https://blog.featurelabs.com>, 2019.
- [34] Q. A. Al-Haija, M. Smadi, S. Zein-Sabatto, "Multi-Class Weather Classification Using ResNet-18 CNN for Autonomous IoT and CPS Applications" in *Proc. Of IEEE 7<sup>th</sup> Annual Conference on Computational Science & Computational Intelligence (CSCI'20)*, Las Vegas, USA, 2020.
- [35] K.E. Koech, "Cross-Entropy Loss Function", Medium: towards data science, 2020.
- [36] A. I. Piriu, M. Leonte, N. Postolachi and D. T. Gavrilut, "Optimizing Cleanset Growth by Using Multi-Class Neural Networks," in *Proc. Of 20<sup>th</sup> International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, Romania, pp. 425-429, 2018.
- [37] A. Banjongkan, et. al., "A Comparative Study of Learning Techniques with Convolutional Neural Network Based on HPC-Workload Dataset" *Inter. Journal of Machine Learning and Computing*, vol. 10, no.1, 2020.
- [38] S. Allagi and R. Rachh, "Analysis of Network log data using Machine Learning," in *Proc. Of IEEE 5<sup>th</sup> International Conference for Convergence in Technology*, India, pp. 1-3, 2019.