IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Prediction of Cyber-Attacks Using Data Science Techniques

Mr. Sudarsanam[1], Sudharsan M[2], Sakthivell V[3], Sakthi Vignesh P[4], Raghavendra Rao D[5]
Assistant Professor, Department of Cyber Security[1]
UG Scholor, Department of Computer Science and Engineering[2,3,4,5]
SRM Valliammai Engineering College, Chengalpattu, India

Abstract: *Cyber-attacks aim to destroy or maliciously manipulate a computing environment or infrastructure, as well as disrupt data integrity or crack all information. This poses a risk to the organisation, perhaps resulting in data loss. The data from device sensors is collected as big data, which has a wealth of information that can be utilised for targeted assaults. Although existing methodologies, models, and algorithms have given the foundation for cyber-attack predictions, new models and algorithms based on data representations other than task-specific techniques are required. Its non-linear information processing architecture, on the other hand, can be customised to learn alternative data representations of network traffic in order to classify different types of network attacks. In this study, we treat cyber-attack prediction as a classification issue, in which networking sectors must use machine learning approaches to forecast the type of network assault from a given dataset. The supervised machine learning technique (SMLT) is used to analyse a dataset in order to capture multiple pieces of information, such as variable identification, uni-variate analysis, bi-variate and multi-variate analysis, missing value treatments, and so on. A comparison of machine learning algorithms was conducted to evaluate which algorithm is the best accurate at predicting the types of cyber-attacks. DOS Attack, R2L Attack, U2R Attack, and Probe Attack are the four types of attacks we classify. The findings reveal that the suggested machine learning algorithm technique has the best accuracy with entropy calculation, precision, recall, F1 Score, sensitivity, specificity, and entropy calculation.*

Keywords: Cyber-attack, DOS Attack, R2L Attack, U2R Attack, Probe Attack

REFERENCES

[1]. Wentao Zhao, Jianping Yin and Jun Long , 2008, A Prediction Model of DoS Attack's Distribution Discrete Probability.
[2]. Preetish Ranjan, Abhishek Vaish, 2014, Apriori Viterbi Model for Prior Detection of Socio-Technical Attacks in a Social Network.
[3]. Seraj Fayyad, Cristoph Meinel, 2013, New Attack Scenario Prediction Methodology
[4]. Jinyu W1, Lihua Yin and Yunchuan Guo, 2012, Cyber Attacks Prediction Model Based on Bayesian Network.
[5]. Xiaoyong Yuan , Pan He, Qile Zhu, and Xiaolin Li, 2019, Adversarial Examples: Attacks and Defenses for Deep Learning.
[6]. Wenying Xu, Guoqiang Hu, 2019, Distributed Secure Cooperative Control Under Denial-of-Service Attacks From Multiple Adversaries.
[7]. Zhen Yang, Yaochu Jin, Fellow, and Kuangrong Hao , 2018, A Bio-Inspired Self-learning Coevolutionary Dynamic Multiobjective
[8]. K. Xu, W. Hu, J. Leskovec, and S. Jegelka, "How powerful are graph neural networks?" in Proc. Int. Conf. Learn. Represent., 2019, pp. 1–17.
[9]. Z. Ying, J. You, C. Morris, X. Ren, W. Hamilton, and J. Leskovec, "Hierarchical graph representation learning with differentiable pooling," in Proc. Adv. Neural Inf. Process. Syst., 2018, pp. 4800–4810.
[10]. M. Zhang and Y. Chen, "Weisfeiler-lehman neural machine for link prediction," in Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Aug. 2017, pp. 575–583.
[11]. T. N. Kipf and M. Welling, "Variational graph auto-encoders," 2016, arXiv:1611.07308.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

[12]. G. Pang, C. Shen, L. Cao, and A. van den Hengel, "Deep learning for anomaly detection: A review," 2020, arXiv:2007.02500.

[13]. K. Ding, J. Li, R. Bhanushali, and H. Liu, "Deep anomaly detection on attributed networks," in Proc. SIAM Int. Conf. Data Mining. Philadelphia, PA, USA: SIAM, 2019, pp. 594–602.

[14]. Y. Chen, X. Sean Zhou, and T. S. Huang, "One-class SVM for learning in image retrieval," in Proc. Int. Conf. Image Process., vol. 1, 2001, pp. 34–37.

[15]. X. Xu, N. Yuruk, Z. Feng, and T. A. J. Schweiger, "SCAN: A structural clustering algorithm for networks," in Proc. 13th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD), 2007, pp. 824–833.

[16]. B. Perozzi and L. Akoglu, "Scalable anomaly ranking of attributed neighborhoods," in Proc. SIAM Int. Conf. Data Mining, Jun. 2016, pp. 207–215.

[17]. J. Li, H. Dani, X. Hu, and H. Liu, "Radar: Residual analysis for anomaly detection in attributed networks," in Proc. 26th Int. Joint Conf. Artif. Intell., Aug. 2017, pp. 2152–2158.

[18]. Z. Peng, M. Luo, J. Li, H. Liu, and Q. Zheng, "ANOMALOUS: A joint modeling approach for anomaly detection on attributed networks," in Proc. 27th Int. Joint Conf. Artif. Intell., Jul. 2018, pp. 3513–3519.

[19]. G. Pang, C. Shen, H. Jin, and A. van den Hengel, "Deep weaklysupervised anomaly detection," 2019, arXiv:1910.13601.

[20]. G. Pang, C. Shen, and A. van den Hengel, "Deep anomaly detection with deviation networks," in Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Jul. 2019, pp. 353–362.

[21]. L. Ruff et al., "Deep one-class classification," in Proc. Int. Conf. Mach. Learn., 2018, pp. 4393–4402.

[22]. Y. Li, X. Huang, J. Li, M. Du, and N. Zou, "SpecAE: Spectral AutoEncoder for anomaly detection in attributed networks," in Proc. 28th ACM Int. Conf. Inf. Knowl. Manage., Nov. 2019, pp. 2233–2236.