Método de detección de ataques basado en el modelo de red neuronal convolucional y el conjunto de datos "inSDN"

1.Contexto de aplicación.
Información adicional para IDS consultar [8], [9] y [10]; información adicional para SDN consultar [11], [12] y [13]; información adicional para estadísticas de ciberataques consultar [14], [15] y [16]

2.Objetivo de machine learning (queremos predecir X, dada tal información)

3.Dataset: tipo de datos, tamaño (número de datos y tamaño en disco), distribución de las clases [17]

4.Métricas de desempeño (de machine learning y negocio)

5.Resultados previos

[1], [2], [3], [4], [5], [6], [7]

6.Referencias

[1] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair and F. E. A. El-Samie, "An Efficient Intrusion Detection System for SDN using Convolutional Neural Network," 2021 International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 2021, pp. 1-5, doi: 10.1109/ICEEM52022.2021.9480383.

[2] A. H. Janabi, T. Kanakis and M. Johnson, "Convolutional Neural Network Based Algorithm for Early Warning Proactive System Security in Software Defined Networks," in IEEE Access, vol. 10, pp. 14301-14310, 2022, doi: 10.1109/ACCESS.2022.3148134.

[3] M. K, K. K, U. J, P. T, S. AR and S. D, "Classification of DDoS in Software-Defined IoT Networks using Hybrid Feature Selection Technique with DL," 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1-6, doi: 10.1109/ICSTCEE56972.2022.10099827.

[4] Y. Wang, X. Yi, Z. Bao and B. Yu, "An Effective Anomaly Detection Model Combined Feature Selection with Improved CNN in SDN," 2023 3rd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS), Shenyang, China, 2023, pp. 281-287, doi: 10.1109/ACCTCS58815.2023.00048.

[5] H. A. Hassan, E. El-Din Hemdan, M. Shokair, F. E. A. El-Samie and W. El-Shafai, "An Efficient Attack Detection Framework in Software-Defined Networking using Intelligent Techniques," 2023 3rd International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 2023, pp. 1-6, doi:

10.1109/ICEEM58740.2023.10319575.

[6] R. B. Said and I. Askerzade, "Attention-Based CNN-BiLSTM Deep Learning Approach for Network Intrusion Detection System in Software Defined Networks," 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI), Baku, Azerbaijan, 2023, pp. 1-5, doi: 10.1109/PCI60110.2023.10325985.

[7] R. Ben Said, Z. Sabir and I. Askerzade, "CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking With Hybrid Feature Selection," in IEEE Access, vol. 11, pp. 138732-138747, 2023, doi: 10.1109/ACCESS.2023.3340142

[8] A. K. Saxena, S. Sinha and P. Shukla, "General study of intrusion detection system and survey of agent based intrusion detection system," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 471-421, doi: 10.1109/CCAA.2017.8229866.

[9] A. R. b. Gupta and J. Agrawal, "A Comprehensive Survey on Various Machine Learning Methods used for Intrusion Detection System," 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 2020, pp. 282-289, doi: 10.1109/CSNT48778.2020.9115764.

[10] A. L. Giri and S. Annamalai, "Intrusion Detection System for Local Networks – A Review Study," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1388-1393, doi: 10.1109/ICACITE53722.2022.9823433.

[11] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[12] B. A. A. Nunes, M. Mendonca, X. -N. Nguyen, K. Obraczka and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617-1634, Third Quarter 2014, doi: 10.1109/SURV.2014.012214.00180.

[13] J. Xie et al., "A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393-430, Firstquarter 2019, doi: 10.1109/COMST.2018.2866942.

[14] https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/

[15] https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

[16] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

[17] M. S. Elsayed, N. -A. Le-Khac and A. D. Jurcut, "InSDN: A Novel SDN Intrusion Dataset," in IEEE Access, vol. 8, pp. 165263-165284, 2020, doi: 10.1109/ACCESS.2020.3022633