IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, June 2023

Brute Force Attacks Detection on IoT Networks using Deep Learning Techniques

Shubham A. Shirodkar
Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application, Mumbai, India
University of Mumbai, Mumbai, India
shubhamshiro373@gmail.com

Abstract: *The Internet of Things (IoT) sector is expanding quickly, and its applications are becoming more prevalent in our day-to-day lives. Various protocols are used to control communication between IoT devices. The Message Queue Telemetry Protocol (MQTT), a simple and trustworthy communication protocol, is a well-known illustration of these protocols. However, MQTT-IoT networks have been the target of cyberattacks, which highlights the need for an effective intrusion detection system for spotting such attempts. The brute force attack is a common sort of such attacks. We suggest deep learning in this study as a means of automatically identifying brute force assaults on MQTT-IoT networks. We train the deep learning model with a large number of instances and a flow-based feature using the MQTT-IoT-IDS2020 dataset. With more than 99% accuracy in differentiating between regular and brute force attacks, the classification model is quite accurate in detecting such attempts.*

Keywords: Internet of Things

REFERENCES

[1] Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., & Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. Internet of Things,16,100264.
[2] https://iot-analytics.com/number-connected-iot-devices/,accesses1-5-2022.
[3] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. Ieee Access, 8, 23022-23040.
[4] Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., Yan, C. (2020). Investigating messaging protocols for the Internet of Things (IoT). IEEE Access, 8, 94880-94911.
[5] Naik, N. (2017, October). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE international systems engineering symposium (ISSE) (pp. 1-7). IEEE.
[6] Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., ... Buchanan, W. J. (2021). A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT. Sensors, 21(21), 7016.
[7] Singh, M., Rajan, M. A., Shivraj, V. L., Balamuralidhar, P. (2015, April). Secure mqtt for internet of things (iot). In 2015 fifth international conference on communication systems and network technologies (pp. 746-751). IEEE.
[8] Alani, M. M. (2018, December). IoT lotto: Utilizing IoT devices in brute-force attacks. In Proceedings of the 6th International Conference on Information Technology: IoT and Smart City (pp. 140-144).
[9] Najafabadi, M. M., Khoshgoftaar, T. M., Kemp, C., Seliya, N., Zuech, R. (2014, November). Machine learning for detecting brute force attacks at the network level. In 2014 IEEE International Conference on Bioinformatics and Bioengineering (pp. 379-385). IEEE.
[10] Perrone, G., Vecchio, M., Pecori, R., Giaffreda, R. (2017, April). The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-attack Carried Out through an Army of IoT Devices. In IoTBDS (pp. 246-253).
[11] Hindy, H., Bayne, E., Bures, M., Atkinson, R., Tachtatzis, C., Bellekens, X. (2020, September). Machine learning based IoT intrusion detection system: an MQTT case study (MQTT-IoT-IDS2020 dataset). In International Networking Conference (pp. 73-84). Springer, Cham.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, June 2023

[12] Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.
[13] Canedo, J., Skjellum, A. (2016, December). Using machine learning to secure IoT systems. In 2016 14th annual conference on privacy, security and trust (PST) (pp. 219-222). IEEE.
[14] Alaiz-Moreton, H., Aveleira-Mata, J., Ondicol-Garcia, J., Muñoz-Castañeda, A. L., García, I., Benavides, C. (2019). Multiclass classification procedure for detecting attacks on MQTT- IoT protocol. Complexity, 2019.
[15] Syed, N. F., Baig, Z., Ibrahim, A., Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. Journal of Information and Telecommunication, 4(4), 482-503.
[16] Ciklabakkal, E., Donmez, A., Erdemir, M., Suren, E., Yilmaz, M. K., Angin, P. (2019, October). ARTEMIS: An intrusion detection system for MQTT attacks in Internet of Things. In 2019 38th Symposium on Reliable Distributed Systems (SRDS) (pp. 369-3692). IEEE.