*Network and Computer Applications*, vol. 163, no. April, 2020, doi:10.1016/j.jnca.2020.102662.

[39] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," *Arab J Sci Eng*, 2021, doi: 10.1007/s13369-021-06086-5.

[40] M. T. Banday, J. A. Qadri, and N. A. Shah, "Study of Botnets and their threats to Internet Security," *Working Papers on Information Systems*, no. January 2009, 2009.

[41] M. Eslahi, R. Salleh, and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," *Proceedings - 2012 IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2012*, no. November, pp. 349–354, 2012, doi:10.1109/ICCSCE.2012.6487169.

[42] A. Kak, "Lecture Notes on ' Computer and Network Security ' Goals : Section Title," pp. 1–82, 2020.

[43] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: A classification," *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2003*, no. June 2014, pp. 190–193, 2003, doi:10.1109/ISSPIT.2003.1341092.

[44] M. A. Raza, T. F. N. Bukht, M. Ali, A. U. Rehman, and M. Idrees, "Analyzing the Behaviour of DDoS Cyber Attack," *Technical Journal*, vol. 26, no. 4, pp. 46–55, 2021.

[45] K. K. Brahma, S. Sarmah, C. Kalita, and R. Ghosh, "Detection of Multi-Vector DDoS Attack International Journal of Computer Sciences and Engineering Open Access Detection of Multi-Vector DDoS Attack," no. December, 2019.

[46] W. Niu, X. Zhang, X. Du, L. Zhao, R. Cao, and M. Guizani, "A deep learning based static taint analysis approach for IoT software vulnerability location," *Measurement (Lond)*, vol. 152, p. 107139, 2020, doi: 10.1016/j.measurement.2019.107139.

[47] M. A. Azad, F. Riaz, A. Aftab, S. K. J. Rizvi, J. Arshad, and H. F. Atlam, "DEEPSEL: A novel feature selection for early identification of malware in mobile applications," *Future Generation Computer Systems*, vol. 129, pp. 54–63, 2022, doi: 10.1016/j.future.2021.10.029.

[48] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for Internet of Things," *Computer Networks*, vol. 186, no. January, p. 107784, 2021, doi: 10.1016/j.comnet.2020.107784.

[49] H. K. Bui, Y. D. Lin, R. H. Hwang, P. C. Lin, V. L. Nguyen, and Y. C. Lai, "CREME: A toolchain of automatic dataset collection for machine learning in intrusion detection," *Journal of Network and Computer Applications*, vol. 193, no. August, p. 103212, 2021, doi:10.1016/j.jnca.2021.103212.

[50] M. Chowdhury, B. Ray, S. Chowdhury, and S. Rajasegarar, "A Novel Insider Attack and Machine Learning Based Detection for the Internet of Things," *ACM Transactions on Internet of Things*, vol. 2, no. 4, pp. 1–23, 2021, doi: 10.1145/3466721.

[51] F. Ullah, M. R. Naeem, A. S. Bajahzar, and F. Al-Turjman, "IoT-based Cloud Service for Secured Android Markets using PDG-based Deep Learning Classification," *ACM Trans Internet Technol*, vol. 22, no. 2, pp. 1–17, 2022, doi: 10.1145/3418206.

[52] Y. S. Can and C. Ersoy, "Privacy-preserving Federated Deep Learning for Wearable IoT-based Biomedical Monitoring," *ACM Trans Internet Technol*, vol. 21, no. 1, 2021, doi: 10.1145/3428152.

[53] J. Chauhan, J. Rajasegaran, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "Performance Characterization of Deep Learning Models for Breathing-based Authentication on Resource-Constrained Devices," *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 2, no. 4, pp. 1–24, 2018, doi: 10.1145/3287036.

[54] J. Danial, D. Das, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "EM-X-DL: Efficient Cross-device Deep Learning Side-channel Attack With Noisy EM Signatures," *ACM J Emerg Technol Comput Syst*, vol. 18, no. 1, pp. 1–17, 2022, doi: 10.1145/3465380.

[55] Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, "AI-empowered IoT Security for Smart Cities," *ACM Trans Internet Technol*, vol. 21, no. 4, 2021, doi: 10.1145/3406115.

[56] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems*, vol. 111, pp. 763–779, 2020, doi:10.1016/j.future.2019.10.015.

[57] N. M, M. H, and K. T, "Virtual Machines Detection Methods Using IP Timestamps Pattern Characteristic," *International Journal of Computer Science and Information Technology*, vol. 8, no. 1, pp. 1–15, 2016, doi: 10.5121/ijcsit.2016.8101.

[58] N. A. M. Razali *et al.*, *Opinion mining for national security: techniques, domain applications, challenges and research opportunities*, vol. 8, no. 1. Springer International Publishing, 2021. doi: 10.1186/s40537-021-00536-5.

[59] W. N. W. Muhamad *et al.*, "Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 12, pp. 597–606, 2020, doi: 10.14569/IJACSA.2020.0111270.

[60] R. Wahyudi, "Metadata of the chapter that will be visualized in Online," *Springer Nature Singapor*, no. August, pp. 1–8, 2023, doi: 10.1007/978-3-030-34032-2.

[61] M. Noorafiza, H. Maeda, R. Uda, T. Kinoshita, and M. Shiratori, "Vulnerability analysis using network timestamps in full virtualization virtual machine," *ICISSP 2015 - 1st International Conference on Information Systems Security and Privacy, Proceedings*, no. January 2015, pp. 83–89, 2015, doi: 10.5220/0005242000830089.