**REFERENCES**

[1] Vibekananda Dutta , Michał Chora´s, Marek Pawlicki and Rafał Kozik, "A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection", Sensors, August 2020.

[2] Quoc-Dung Ngo, Huy-Trung Nguyen, Van-Hoang Le, Doan-Hieu Nguyen, "A survey of IoT malware and detection methods based on static features", ICT Express, December 2020.

[3] Hui Wu, Haiting Han, Xiao Wang, and Shengli Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey", IEEE Access, August 2020.

[4] Shakila Zaman, Khaled Alhazmi, Mohammed A. Aseeri, Muhammad Raisuddin Ahmed, Risala Tasin Khan, M. Shamim Kaiser and Mufti Mahmud, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey", IEEE Access, June 2021.

[5] Benjamin Vignau, Raphaël Khoury, Sylvain Hallé, Abdelwahab Hamou-Lhadj, "The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives", J. Syst. Archit., June 2021.

[6] Nicolas-Alin Stoian, "Machine Learning for Anomaly Detection in IoT networks: Malware analysis on the IoT-23 Data set", University of Twente, 2020.

[7] Al-Zewairi, Malek, Sufyan Almajali, and Moussa Ayyash. "Unknown Security Attack Detection Using Shallow and Deep ANN Classifiers." Electronics 9.12, November 2020

[8] Ullah, Imtiaz, and Qusay H. Mahmoud. "Network Traffic Flow Based Machine Learning Technique for IoT Device Identification." IEEE International Systems Conference (SysCon), 2021

[9] Booij, Tim M., et al. "ToN\_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Datasets." IEEE Internet of Things Journal, May 2021.

[10] Cai, Yun‐Zhan, et al. "E‐Replacement: Efficient scanner data collection method in P4 ‐ based software ‐ defined networks." International Journal of Network Management, November 2021

[11] Tian, Pu, et al. "Towards Asynchronous Federated Learning Based Threat Detection: a DC-Adam Approach." Computers & Security, Sep 2021

[12] Kalinin, Maxim O., V. M. Krundyshev, and B. G. Sinyapkin. "Development of the Intrusion Detection System for the Internet of Things Based on a Sequence Alignment Algorithm." Automatic Control and Computer Sciences 54.8, Dec 2020

[13] Daniel K. Andrews; Rajeev K. Agrawal; Suzanne J. Matthews; Alexander S. Mentis. "Comparing Machine Learning Techniques for Zeek Log Analysis", IEEE Xplore, January 2022

[14] Steffen Haas, Robin Sommer & Mathias Fischer. "Zeek-Osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection", IFIPAICT, Sep 2020

[15] Gustavsson, Vilhelm. “Machine Learning for a Network-based Intrusion Detection System : An application using Zeek and the CICIDS2017 dataset.”, 2019.

[16] Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions", Mobile Networks and Applications, 1-17, 2022

[17] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review", Electronics, 11(2), 198, 2022