Challenges and solutions on the use of Artificial Intelligence in Internet of Things network security

Svetlana Cojocaru, Ludmila Peca
Technical University of Moldova, 168, Stefan cel Mare și Sfant Blvd., Chisinau, MD-2004, Republic of Moldova, svetlana.cojocaru@ati.utm.md, ludmila.peca@isa.utm.md, ORCID: 0000-0002-1187-4294, 0000-0002-4394-2933, https://utm.md/

Keywords: artificial intelligence, cyber security, Internet of Things networks, anomaly detection, cyber-attacks, machine learning

Abstract. The article is an analysis of how artificial intelligence can be used for the security of Internet of Thinks networks, emphasizing its use in the detection and prevention of cyber-attacks.

The article focuses on new advances in the use of artificial intelligence for: anomaly detection through machine learning algorithms; automating response processes by reducing incident response time by isolating compromised devices; detecting suspicious activity by strengthening protection against attacks.

Recent research results showing the effectiveness of Artificial Intelligence in securing the Internet of Things have been analyzed: the use of machine learning algorithms to detect DDoS attacks on Internet of Things devices, the implementation of autoencoding for botnet detection, the highlighting of vulnerabilities of unsecured Internet of Things devices and the integration of Artificial Intelligence in security, the development of an intrusion detection system based on recurrent neural networks for Internet of Things networks.

The analysis shows that Artificial Intelligence implementation offers solutions for detecting and preventing cyber-attacks, but there are also challenges related to data quality, detection errors and implementation complexity.

To overcome these, new research directions are recommended: development of algorithms to reduce false alarms, Artificial Intelligence assisted security, data protection by training Artificial Intelligence models directly on Internet of Things devices, use of deep learning to identify and neutralize unknown threats.

References

[1] M. Antonakakis, T. April, M. BArtificial Intelligenceley, E. Bursztein, et al., Understanding the MirArtificial Intelligence Botnet, in Proceedings of the 26th USENIX Security Symposium. (2017) 1093–1110.

[2] R. Doshi, N. Apthorpe, N. Feamster, Machine Learning DDoS Detection for Consumer Internet of Things Devices, in Proceedings of the IEEE Security and Privacy Workshops (SPW). (2018) 29–35.

[3] Y. Meidan, M. Bohadana, A. ShabtArtificial Intelligence, J. Guarnizo, et al., N-BArtificial Intelligencenternet of Things —Network-based Detection of Internet of Things Botnet Attacks Using Deep Autoencoders, IEEE Pervasive Computing. 17 (2018) 12–22.

[4] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, Security, Privacy and Trust in Internet of Things: The Road Ahead, Computer Networks. 76 (2015) 146–164.

[5] E. Fernandes, J. Jung, A. Prakash, Security Analysis of Emerging Smart Home Applications, in Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). (2016) 636–654.