ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 12, December 2021 SJIF 2021 = 7.492
A peer reviewed journal

AN OVERVIEW OF THE USAGE OF ARTIFICIAL INTELLIGENCE-BASED INTRUSION DETECTION METHODS

Dr. Vinay Kumar Mishra*

*Associate Professor,
Department of Computer Science, Faculty of Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: vinaym.computers@tmu.ac.in

DOI: 10.5958/2249-7137.2021.02666.5

ABSTRACT

Huge numbers of computer across the globe, operating on a variety of hardware or software platforms, link to provide communication and commercial services over the Internet. However, since computers are interconnected, malevolent individuals may abuse resources and launch Internet assaults. The ever-increasing number of Internet assaults makes it difficult to create flexible, adaptable security solutions. One of the most significant components used to identify Internet assaults is the intrusion detection system (IDS). Various methods from various disciplines have been used in the literature to create effective IDS. Artificial intelligence (AI)-based methods have an important part in the development of IDS as well as provide many advantages over other approaches. There is, however, no thorough evaluation of AI-based methods to evaluate and comprehend their present position in solving intrusion detection issues. Various AI-based methods have been discussed in this article, with an emphasis on IDS creation. The sources of data sets, processing criteria, method utilized, dataset, classifier design, dimension reduction technique used, and other experimental environment setup have all been compared. The advantages and disadvantages of AI-based methods were addressed. The article will aid in a better understanding of the many avenues in which IDS research has been conducted. The results of this article are helpful for individuals interested in applying AI-based methods to IDS and related areas, since they offer important insights into the literature. The study also discusses the research's future directions in this field.

KEYWORDS: *Artificial Intelligence, Ensemble System, Hybrid System, Intrusion Detection System, Intrusion, Network Security.*

REFERENCES

1. M. Alkasassbeh, “An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods,” J. Theor. Appl. Inf. Technol., 2017.
2. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” 2017, doi: 10.1109/ICOIN.2017.7899588.
3. G. Kumar, K. Kumar, and M. Sachdeva, “The use of artificial intelligence based techniques for intrusion detection: A review,” Artif. Intell. Rev., 2010, doi: 10.1007/s10462-010-9179-5.

4. Z. Jinbiao, "Research on intrusion detection system based on clustering fuzzy support vector machine," Int. J. Secur. its Appl., 2014, doi: 10.14257/ijsia.2014.8.3.26.

5. J. Kusyk, M. U. Uyar, and C. S. Sahin, "Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks," Evol. Intell., 2018, doi: 10.1007/s12065-018-0154-4.

6. V. K. Pachghare, V. A. Patole, and D. P. Kulkarni, "Self Organizing Maps to Build Intrusion Detection System," Int. J. Comput. Appl., 2010, doi: 10.5120/191-328.

7. D. KS and B. Ramakrishna, "An Artificial Neural Network based Intrusion Detection System and Classification of Attacks," Int. J. Eng. Res. Appl., 2013.

8. G. Kumar and K. Kumar, "The Use of Artificial-Intelligence-Based Ensembles for Intrusion Detection: A Review," Appl. Comput. Intell. Soft Comput., 2012, doi: 10.1155/2012/850160.

9. Y. Gao, Y. Liu, Y. Jin, J. Chen, and H. Wu, "A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System," IEEE Access, 2018, doi: 10.1109/ACCESS.2018.2868171.

10. C. Guo, Y. J. Zhou, Y. Ping, S. S. Luo, Y. P. Lai, and Z. K. Zhang, "Efficient intrusion detection using representative instances," Comput. Secur., 2013, doi: 10.1016/j.cose.2013.08.003.