INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES

ISSN: 2322-0821(O)
ISSN: 2394-9910(P)

VOLUME 12 ISSUE 2
April 2024 - June 2024

www.irjeas.org

Original Article

Enhancing Intrusion Detection Performance Through Deep Learning Method

Bhawana Choudhary [1], Dr. P.K Sharma [2]

[1] *M. Tech Scholar, Computer Science & Engineering Department, NRI Institute of Research and Technology Bhopal*
bhawanachoudhary61@gmail.com
[2] *Associate Professor & HOD, Computer Science & Engineering Department, NRI Institute of Research and Technology Bhopal*
principal.nirt@gmail.com

Corresponding Author: bhawanachoudhary61@gmail.com

DOI –10.55083/irjeas.2024.v12i02004

Abstract: In the realm of cyber and data security, the field of intrusion detection systems (IDS) stands out as an area of active research. Traditional methods, such as data mining, statistical evaluation, and artificial neural networks, face significant challenges in achieving accurate intrusion detection. However, the emergence of machine learning algorithms offers promising solutions to this challenge. This paper presents a novel approach to intrusion detection, focusing on leveraging deep learning methodologies. Deep learning, as an extension of machine learning, holds the potential to enhance the accuracy of IDS. The proposed method employs a cascaded three-level convolutional neural network (CNN) architecture. Efficiency and scalability in intrusion detection hinge upon effective feature reduction. By streamlining features, the capacity for intrusion classification and attack detection is significantly enhanced. Notably, when applied to datasets like KDDCUP99 with diverse attributes, the proposed algorithm achieves a detection ratio nearing 100%, albeit with a slightly lower classification ratio due to attribute diversity. Comparative analysis demonstrates the superiority of the cascaded CNN algorithm over traditional CNN methods in both feature reduction and classification tasks. Particularly, the proposed algorithm showcases remarkable efficiency in handling dynamic attributes, thereby improving classification accuracy. the proposed approach utilizing cascaded CNN architecture presents a substantial advancement in intrusion detection and classification compared to conventional methods. Through the integration of deep learning techniques, this methodology offers a robust solution to the challenges encountered in traditional intrusion detection systems.

Keywords: - IDS, CNN, KDDCUP2003, Feature Selection, Classification

1. INTRODUCTION

The global expansion of digitalization has interconnected the world into a single platform known as the cyber world. This encompassing digital realm includes all tools and platforms utilized for data sharing and transmission over the internet. However, the exchange of data within this vast information highway necessitates robust security systems to ensure the integrity and authentication of data. In response to these challenges, Anderson developed an intrusion detection system (IDS) in 1980, marking a significant milestone in cybersecurity research. Today, IDS remains one of the most widely employed methods for detecting various forms of malicious attacks within network environments. Deep learning techniques, such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM), have demonstrated remarkable effectiveness across diverse domains, including natural language processing, computer vision, and speech recognition. Our study introduces a unified model called Multiscale Convolutional Neural Network with Long Short-Term Memory (MSCNN-LSTM), which integrates spatial-temporal information for intrusion detection purposes. CNN and LSTM, being prominent deep learning algorithms, excel in extracting spatial and temporal properties from datasets, respectively. While CNN primarily focuses on spatial feature extraction and has shown significant advancements in computer vision tasks, LSTM incorporates self-connected memory units to capture temporal dependencies within sequences. The synergy between these techniques enables the MSCNN-LSTM model to effectively handle intrusion detection challenges by leveraging both spatial and temporal characteristics of intrusion data. The complexity of intrusion data poses challenges for detection performance, emphasizing the need for feature reduction techniques. In this dissertation, we explore the utilization of CNN algorithms for feature reduction in intrusion detection systems. By prioritizing essential features and eliminating redundant ones, we aim to enhance the efficiency of IDS without compromising detection accuracy. this paper presents a comprehensive investigation into the application of deep learning techniques, particularly CNN and LSTM, for intrusion detection. The proposed MSCNN-LSTM model demonstrates promising capabilities in extracting spatial-temporal features crucial for effective intrusion detection. Additionally, our exploration of CNN-based feature reduction techniques offers insights into optimizing IDS performance. The subsequent sections of the paper delve into related work, proposed methodology, experimental analysis, and conclude with future research directions.

2. RELATED WORK

As cyber-attacks become more sophisticated, security has become a top priority in computer networks. Furthermore, as a result of the introduction of technologies such as the cloud, networks are exposed to a variety of invasive activities, resulting in serious degradation. They can also inflict massive monetary losses and have a negative influence on critical IT infrastructure, resulting in data insufficiency in cyberwar [10, 11, 12, 13, 14, and 15]. As a result, security methods must be included to ensure that the system's security is not jeopardized. A secure system's goal is to detect anomalies so that valuable information can be safeguarded. Despite the use of safety features such as firewalls and encryption techniques, various attacks have been discovered that overcome the system's security protections. As a result, it is crucial to detect them as soon as possible in order to minimize the risk of harm to critical resources, and appropriate actions can then be taken to eliminate the incursion. Because of its robustness, an intrusion detection system (IDS) is the most potent tool for detecting unwanted attempts to access, manipulate, or disable a computer system, mostly via the internet. It analyses incoming and outgoing traffic for malicious activity that could compromise the system's security. As a result, it is a necessary tool for network administrators because it is impossible to inspect a massive volume of data travelling the network every second without such a device. A MIDS and an anomaly intrusion detection system are two types of intrusion detection systems (AIDS) [18, 19, 20]. Misuse detection compares the user's activity to known attack signatures, and if a match is found, the associated action is labelled as an attack, whereas in the latter, any deviation from regular behaviour is labelled as an attack. AIDS is unable to identify new sorts of attacks. They do, however, have a lower detection rate than MIDS. In addition, a suitable dataset must be available to evaluate the performance of IDS so that the system's performance may be analysed before it is deployed in the real world. As a result, researchers use a dataset to train and evaluate their model. However, it remains a challenge because only a few datasets are publicly available, and a few of them are incomplete and insufficient. KDD-99, NSL-KDD, UNSW-15, and Botnet are some of the most often used datasets for intrusion detection. Misjudgement, false detection, and a lack of real-time response are the key challenges of IDS. Machine learning (ML) is currently undergoing enormous progress as a result of the capacity of computer devices. As a result, because ML classifiers greatly improve the system's accuracy and robustness, they're being used in the security arena to report numerous attacks. For feature selection and classification of network data, researchers have recently used ML methods such as SVM, DT, MLP, KNN, and RF.

3. PROPOSED METHODOLOGY

The proposed algorithm of intrusion detection system using the principle of flow content of data. the proposed CNN model encompasses M=3. The design of class normal and abnormal of traffic data of intrusion. The activation function of algorithm is RLU and their basic value is 1. The processing of algorithm describes here [26, 27]. the network define relationship between two non-linear variables K and Ki+1 through network function as

$$Ki + 1 = \delta(wki + b) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where δ is activation function and matrix W and b is called model parameters. The variable K and ki+1 is from of layers. the multilayer neural network argumenta with advance learning called deep neural network. The classification of network defines as y=f(u). the process of network function defines as

$$K1= \delta 1(w1u+b1)$$

$$K2= \delta 2(w2p1+b2)$$

$$Y= \delta L(wLpL\text{-}1+bL)$$

Where L is number of layersProcess of training of CNN.

The relation of neurons defines the process of traffic data

$$T_k : X^{n_x} \rightarrow C^{n_x}, \text{ where } x_k \in T^{n_x}$$

Be the set of traffic data in neurons for the processing.

Hypothesis of error estimated by E

$$E_j = H_j(x_j) + v_j, \quad \forall\, k \leq j \leq k + A$$

Where $H_j: R^{n_x} \rightarrow R^{n_y}$ is the relation of multilayer input?

estimate trained pattern

$$x_k = F_0 \rightarrow k(x_0) + \xi k$$

Define learning factor as

$$x_k = arg\min_x \left\{ \|x - x_k\| B_k^{-1} + \sum_{j=k}^{k+A} \left\| H_j F_j(x) - y_j \right\| R_j^{-1} \right\}$$

Algorithm

Define $i = 0$

while $i < L$ do

process the data of intrusion and M is vector of convergence

$$\{x_k \mathrm{I}\, k \in [M \,.\, i, M \,.\, (i + 1)]\}$$

$$x_k = arg\min_x \left\{ \|x - x_k\| P_k^{-1} + \sum_{k}^{k+p} \left\| H_j M_j, (x) \right\| p_j^{-1} \right\}$$

Vote the class of classifier

Class $= \{Fs(x_{k-1}),\ x_k\}$ with $k \in [i.M, (i + 1).M]$

Measure i for next step

end

Output: Accuracy

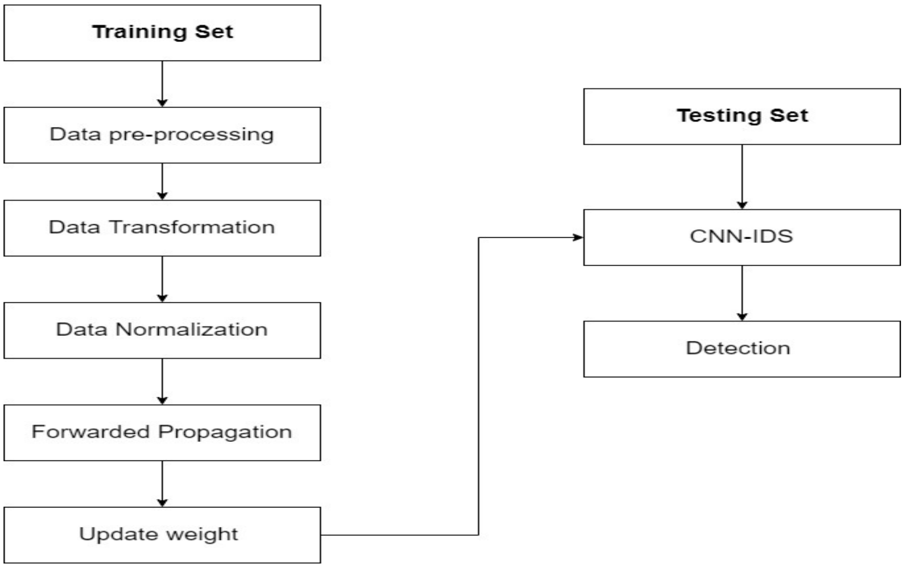

Figure 1: Proposed model of CNN based intrusion detection system

4. EXPERIMENTAL ANALYSIS

To analyzed the performance of machine learning algorithm for intrusion detection system using MATLAB software. MATLAB is well-known data and algorithm analysis tools and supported various function of machine learning. The system configuration of machine for the simulation process windows 10 operating system, 16GB RAM and I7 processor. For the analysis of algorithm employed two reputed dataset of intrusion detection systems are KDDCUP2203 and IDS2017. The empirical evaluation of results measure in form of precision, accuracy and recall [30, 31, 32].

Here we observe that the accuracy value of CNN is highest when number of attribute 20 and lowest value of accuracy in CNN when number of attributes is 5 or the accuracy value of ML is highest when number of attributes is 15 and lowest accuracy value in ML when number of attributes is 5. And the accuracy value of proposed method is highest when number of attributes is 15 and the lowest value of accuracy in proposed method is lowest when number of attributes is 5.

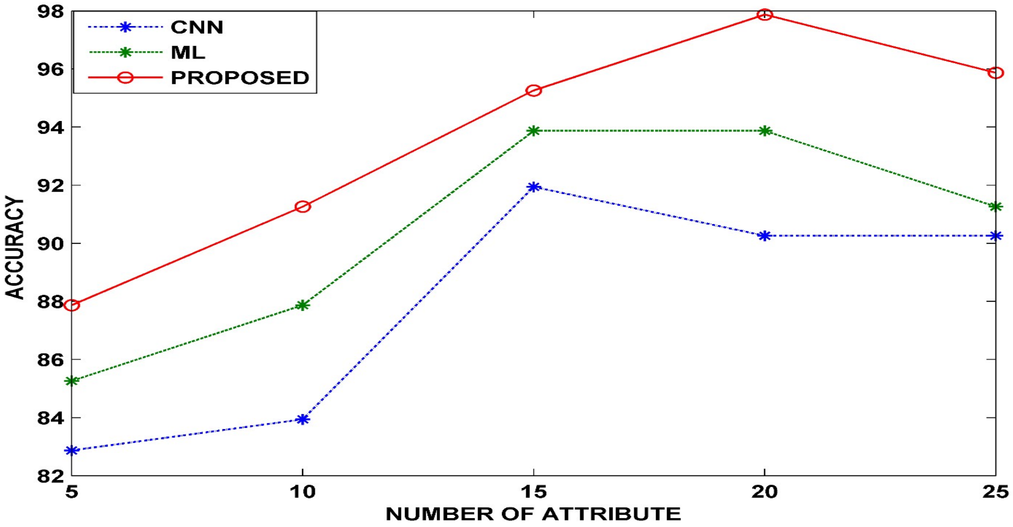

Figure 2: Performance analysis of Accuracy versus Number of attributes.

Here we also observe that proposed method of NSL-KDD dataset is better than other method CNN and ML using accuracy parameter.

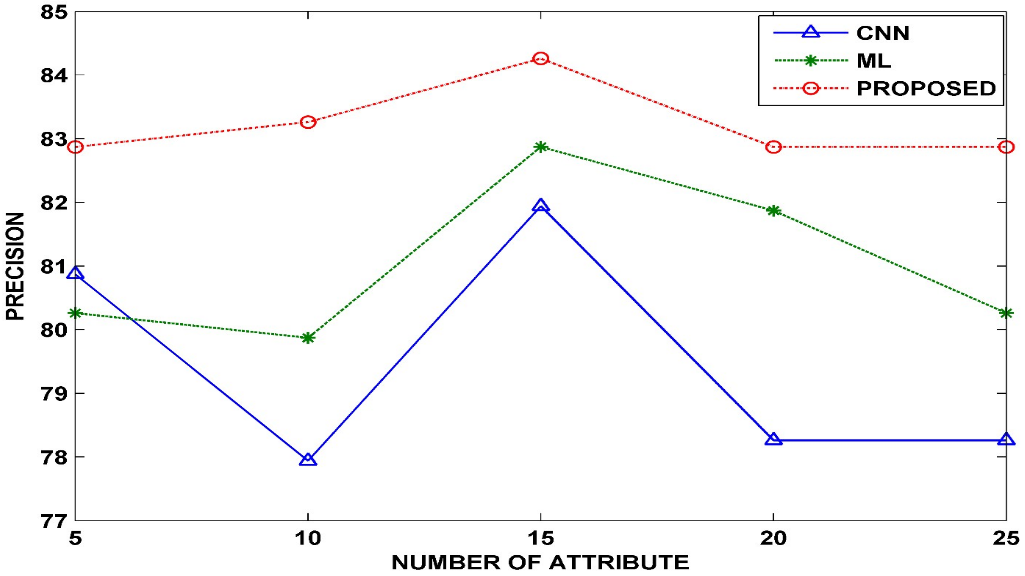

Figure 3: performance analysis of Precision versus Number of attributes.

Here we observe that the Precision value of CNN is highest when number of attribute 15 and lowest value of Precision in CNN when number of attributes is 10 or the Precision value of ML is highest when number of attributes is 15 and lowest Precision value in ML when number of attributes is 10 and the Precision value of proposed method is highest when number of attributes is 15 and the lowest value of Precision in proposed method is lowest when number of attributes is 25.

Here we also observe that proposed method of NSL-KDD dataset is better than other method CNN and ML using Precision parameter.

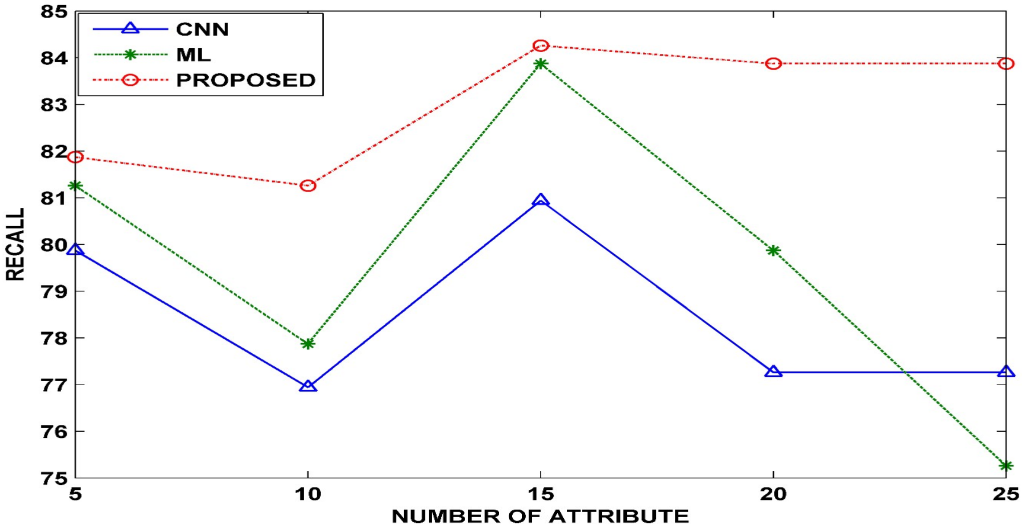

Figure 4: performance analysis of Recall versus Number of attributes

Here we observe that the Recall value of CNN is highest when number of attribute 15 and lowest value of Recall in CNN when number of attributes is 10 or the Recall value of ML is highest when number of attributes is 15 and lowest Recall value in ML when number of attributes is 25 and the Recall value of proposed method is highest when number of attributes is 15 and the lowest value of Recall in proposed method is lowest when number of attributes is 10.

5. CONCLUSION & FUTURE WORK

The subsequent discussion delves into the methodology of machine learning, examining the strengths and weaknesses of various approaches concerning intrusion detection capability and model complexity. Recent research indicates a prevalent use of Convolutional Neural Network (CNN) methodologies to bolster the performance and efficacy of Network Intrusion Detection Systems (NIDS) in terms of detection accuracy and reducing False Alarm Rates (FAR). Notably, CNN techniques feature prominently in approximately 80% of proposed solutions, with decision tree (dt) and Multilayer Perceptron (MLP) emerging as the most favoured algorithms. Furthermore, analysis reveals that about 70% of the recommended approaches were evaluated using the KDD Cup'99 and NSL-KDD datasets due to the wealth of data available in these repositories. Nevertheless, as these datasets fail to adequately represent recent network threats, the applicability of proposed solutions in real-time scenarios is somewhat limited. To address these limitations and enhance intrusion detection accuracy, this study underscores the importance of bridging research gaps. Specifically, there's a need for improving model performance in detecting low-frequency attacks in real-world environments. Additionally, the exploration of cost-effective strategies to streamline complexity in proposed models is deemed essential for achieving optimal performance in intrusion detection applications.

REFERENCES

[1]. Khan, Farrukh Aslam, Abdu Gumaei, AbdelouahidDerhab, and Amir Hussain. "A novel two-stage deep learning model for efficient network intrusion detection." *IEEE Access* 7 (2019): 30373-30385.

[2]. Zhou, Yuyang, Guang Cheng, Shanqing Jiang, and Mian Dai. "Building an efficient intrusion detection system based on feature selection and ensemble classifier." *Computer networks* 174 (2020): 107247.

[3]. Ahmad, Zeeshan, Adnan Shahid Khan, CheahWaiShiang, Johari Abdullah, and Farhan Ahmad. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches." *Transactions on Emerging Telecommunications Technologies* 32, no. 1 (2021): e4150.

[4]. Mighan, SoosanNaderi, and Mohsen Kahani. "A novel scalable intrusion detection system based on deep learning." *International Journal of Information Security* 20, no. 3 (2021): 387-403.

[5]. Zhao, Ruijie, Jie Yin, ZhiXue, Guan Gui, BamideleAdebisi, TomoakiOhtsuki, HarisGacanin, and Hikmet Sari. "An efficient intrusion detection method based on dynamic autoencoder." *IEEE Wireless Communications Letters* 10, no. 8 (2021): 1707-1711.

[6]. Kanna, P. Rajesh, and P. Santhi. "Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features." *Knowledge-Based Systems* 226 (2021): 107132.

[7]. Xu, Hui, Krzysztof Przystupa, Ce Fang, Andrzej Marciniak, OrestKochan, and MykolaBeshley. "A combination strategy of feature selection based on an integrated optimization algorithm and weighted k-nearest neighbor to improve the performance of network intrusion detection." *Electronics* 9, no. 8 (2020): 1206.

[8]. Shubhodip Sasmal. Smart Data Lakes: International Research Journal of Engineering & Applied Sciences (IRJEAS). 11(3), pp. 13-19, 2023. 10.55083/irjeas.2023.v11i04003.

[9]. Mulyanto, Mulyanto, Muhamad Faisal, SetyaWidyawanPrakosa, and Jenq-ShiouLeu. "Effectiveness of focal loss for minority classification in network intrusion detection systems." *Symmetry* 13, no. 1 (2020): 4.

[10]. Ren, Jiadong, JiaweiGuo, Wang Qian, Huang Yuan, Xiaobing Hao, and Hu Jingjing. "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms." *Security and Communication Networks* 2019 (2019).

[11]. Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and JoarderKamruzzaman. "Survey of intrusion detection systems: techniques, datasets and challenges." *Cybersecurity* 2, no. 1 (2019): 1-22.

[12]. Khare, Neelu, Preethi Devan, Chiranji Lal Chowdhary, Sweta Bhattacharya, Geeta Singh, Saurabh Singh, and Byungun Yoon. "SMO-DNN: spider monkey optimization and deep neural network hybrid classifier model for intrusion detection." *Electronics* 9, no. 4 (2020): 692.

[13]. Dwivedi, Shubhra, Manu Vardhan, and SarsijTripathi. "Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection." *Cluster Computing* 24, no. 3 (2021): 1881-1900.

[14]. Shubhodip Sasmal. Real-time Data Processing with Machine Learning Algorithms. International Research Journal of Engineering & Applied Sciences (IRJEAS). 11(4), pp. 91-96, 2023. 10.55083/irjeas.2023.v11i04012.

[15]. Alamiedy, TaiefAlaa, Mohammed Anbar, Zakaria NM Alqattan, and Qusay M. Alzubi. "Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm." *Journal of Ambient Intelligence and Humanized Computing* 11, no. 9 (2020): 3735-3756.

[16]. Devan, Preethi, and Neelu Khare. "An efficient XGBoost–DNN-based classification model for network intrusion detection system." *Neural Computing and Applications* 32, no. 16 (2020): 12499-12514.

[17]. Parsamehr, Reza, Georgios Mantas, Jonathan Rodriguez, and José-Fernán Martínez-Ortega. "Idlp: an efficient intrusion detection and location-aware prevention mechanism for network coding-enabled mobile small cells." *IEEE Access* 8 (2020): 43863-43875.

[18]. Gauthama Raman, M. R., NivethithaSomu, SahrudayJagarapu, Tina Manghnani, ThirumaranSelvam, Kannan Krithivasan, and V. S. Shankar Sriram. "An efficient intrusion detection technique based on support vector machine and improved binary gravitational search algorithm." *Artificial Intelligence Review* 53, no. 5 (2020): 3255-3286.

[19]. Upasani, Nilam, and Hari Om. "A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection." *Applied Soft Computing* 82 (2019): 105595.

[20]. Krishnaveni, S., S. Sivamohan, S. S. Sridhar, and S. Prabakaran. "Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing." *Cluster Computing* 24, no. 3 (2021): 1761-1779.

[21]. Papamartzivanos, Dimitrios, Félix Gómez Mármol, and Georgios Kambourakis. "Introducing deep learning self-adaptive misuse network intrusion detection systems." *IEEE Access* 7 (2019): 13546-13560.

[22]. Maseer, ZiadoonKamil, RobiahYusof, Nazrulazhar Bahaman, Salama A. Mostafa, and CikFeresaMohdFoozy. "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset." *IEEE access* 9 (2021): 22351-22370.

[23]. Ghanem, Waheed Ali HM, Aman Jantan, Sanaa Abduljabbar Ahmed Ghaleb, and Abdullah B. Nasser. "An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly

algorithms for training multilayer perceptrons." *IEEE Access* 8 (2020): 130452-130475.

[24]. Almomani, Iman, and AfnanAlromi. "Integrating software engineering processes in the development of efficient intrusion detection systems in wireless sensor networks." *Sensors* 20, no. 5 (2020): 1375.

[25]. Anton, Simon D. Duque, Sapna Sinha, and Hans Dieter Schotten. "Anomaly-based intrusion detection in industrial data with SVM and random forests." In *2019 International conference on software, telecommunications and computer networks (SoftCOM)*, pp. 1-6. IEEE, 2019.

[26]. Magán-Carrión, Roberto, Daniel Urda, Ignacio Díaz-Cano, and BernabéDorronsoro. "Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches." *Applied Sciences* 10, no. 5 (2020): 1775.

[27]. Kaja, Nevrus, Adnan Shaout, and Di Ma. "An intelligent intrusion detection system." *Applied Intelligence* 49, no. 9 (2019): 3235-3247.

[28]. Xu, Hui, Qianqian Cao, Heng Fu, and Hongwei Chen. "Applying an improved elephant herding optimization algorithm with spark-based parallelization to feature selection for intrusion detection." *International Journal of Performability Engineering* 15, no. 6 (2019): 1600

[29]. Gurung, Sandeep, MirnalKantiGhose, and ArojSubedi. "Deep learning approach on network intrusion detection system using NSL-KDD dataset." *International Journal of Computer Network and Information Security* 11, no. 3 (2019): 8-14.

[30]. Sultana, Nasrin, Naveen Chilamkurti, Wei Peng, and RabeiAlhadad. "Survey on SDN based network intrusion detection system using machine learning approaches." *Peer-to-Peer Networking and Applications* 12, no. 2 (2019): 493-501.

[31]. Tang, Chaofei, NurbolLuktarhan, and Yuxin Zhao. "An efficient intrusion detection method based on lightgbm and autoencoder." *Symmetry* 12, no. 9 (2020): 1458.

[32]. Zhou, Yuyang, Guang Cheng, Shanqing Jiang, and Mian Dai. "Building an efficient intrusion detection system based on feature selection and ensemble classifier." *Computer networks* 174 (2020): 107247.

[33]. Hassan, Mohammad Mehedi, Abdu Gumaei, Ahmed Alsanad, MajedAlrubaian, and Giancarlo Fortino. "A hybrid deep learning model for efficient intrusion detection in big data environment." *Information Sciences* 513, p.n. 386-396, 2020.

[34]. Qureshi, Aqsa Saeed, Asifullah Khan, NaumanShamim, and Muhammad HanifDurad. "Intrusion detection using deep sparse auto-encoder and self-taught learning." *Neural Computing and Applications* 32, no. 8, p.n. 3135-3147, 2020.

[35]. Wang, Hui, Zijian Cao, and Bo Hong. "A network intrusion detection system based on convolutional neural network." *Journal of Intelligent & Fuzzy Systems* 38, no. 6, p.n. 7623-7637, 2020.

[36]. Shubhodip Sasmal. Data Warehousing Revolution: AI-driven Solutions. International Research Journal of Engineering & Applied Sciences (IRJEAS). 12(1), pp. 01-06, 2024. 10.55083/irjeas.2024.v12i01001.

Conflict of Interest Statement: *The authors declares that there is no conflict of interest regarding the publication of this paper.*

Cite this Article

Bhawana Choudhary, Dr. P.K Sharma. Enhancing Intrusion Detection Performance through Deep Learning Method. A Comparative Analysis. International Research Journal of Engineering & Applied Sciences (IRJEAS). 12(2), pp. 22-28, 2024.
https://doi.org/10.55083/irjeas.2024.v12i02004