Journal for Technology and Science
Homepage : https://journal.antispublisher.com/index.php/IPTEKS/index
Email : admin@antispublisher.com

e-ISSN : 3047-4337
JOTECH, Vol. 2, No. 3, July 2025
Page 8-18

Evaluating The Security Performance of Using Neural Network in Industrial Internet of Things

Nameer Majid Hashim
Independence Researcher

Check for updates OPEN ACCESS

DOI : https://doi.org/10.61796/ipteks.v2i3.408

Sections Info

Article history:
Submitted: May 20, 2025
Final Revised: Juny 18, 2025
Accepted: July 03, 2025
Published: July 31, 2025

Keywords:
Internet of industrial things
Machine learning
Neural network
Genetic algorithm
Intrusion detection

ABSTRACT

Objective: *The aim of this research is to develop group-based classifications that improve the accuracy of intrusion detection.* ***Method:*** *So far, various methods and algorithms have been presented for data mining, and in this research, machine learning, neural network and optimization of weights with the help of genetic algorithm were used. For this purpose, kdd 99 dataset was used for data preprocessing and Convolutional Neural Network (CNN) algorithm was evaluated along with SVM and KNN algorithms. SVM and KNN algorithms were implemented using R software and convolutional neural network algorithm in MATLAB.* ***Results:*** *The results show that the use of machine learning and the neural system have acceptable results in intrusion detection. However, the weights optimized by the genetic algorithm show higher accuracy than the case with the original weights.* ***Novelty:*** *Comparing these results with the results of previous studies shows that the speed of convergence is much faster, which is one of the advantages of this algorithm.*

INTRODUCTION

Internet of Things (IoT) is a new innovation that has emerged as a big new topic in recent years [1]. The Internet of Things can be described as a system of interconnected objects, mechanical and digital machines, computing devices, and living organisms such as animals and humans, which are provided with unique identifiers (UIDs) in order to transmit data over a network [1,2]. These operations are usually performed without human-computer or human-human interaction [3]. IoT can be used for any device in any branch of science or in any situation, for example, implanting a heart monitor for a person, lightweight sensors in an animal farm, web-connected sensor that improves manufacturing processes, or built-in sensor to inform any and all applications of IoT [4].

This technology provides huge business value to organizations and companies in fields such as industry, health, agriculture, education and tourism [5]. Thus, it provides opportunities for multiple parties (consumers, companies, and governments) to benefit from the features and benefits of this technology. However, the majority of IoT devices are produced without considering security and privacy [6]. Therefore, according to Gartner reports, a large percentage of all devices, i.e. 20 billion devices connected to the Internet of Things in 2020, lack sufficient defense mechanisms to protect them against security attacks, which has a negative impact on the improvement and evolution of this technology [7].

These examples of network intrusion attacks not only disrupt the availability of device functionality, but also involve stealing important information and data about the device and the users who use it. Hence, it is necessary to resist these attacks [8], [9]. This

creates the need for more intelligent mechanisms to connect and use IoT devices [10]. One such mechanism is intrusion detection systems (IDS), which is a software or tool that monitors the network to keep it secure and detect any malicious activity that is taking place. Next, the system reports and collects these violations using event management systems and security information.

Due to the limitations of computing and infrastructure resources, it is difficult to apply traditional security techniques to directly secure IoT devices. Therefore, anomaly-based detection mechanisms are very important with the growth of IoT environments and technology. Big data generation from IoT devices can be useful for machine learning algorithms, where they can perform data analysis and provide meaningful predictions and interpretations of IoT devices. Therefore, the use of machine learning for the security of the Internet of Things system is considered an optimal opportunity to protect them from intrusion attacks, especially by identifying any external activity that appears in the system.

Subject literature studies show that the use of machine learning techniques with Internet of Things intrusion detection methods has received more attention from researchers, however, machine learning itself is classified into different types and studies in this field are still evaluating the methods and improving them. Therefore, in line with the continuation of this research, in this thesis, it has been tried to measure the use of Convolutional Neural Network (CNN) in the security of industrial IoT and its efficiency and performance with other machine learning methods.

RESEARCH METHOD

Related Work in IoT Security

In an article, Liu investigated the security of deep reinforcement learning for the Industrial Internet of Things. In this paper, we first design a DRL-based controller that can be deployed on an edge computing server to enable automatic control in the IIoT context. We then investigate the malicious behaviors of adversaries with two attacks: (1) performance-based attacks that can be launched during the training phase and (b) performance-based attacks that can be launched after the training phase to investigate the security effects of the vulnerable DRL. Based on adversary controllers, Maximum Entropy Inverse Reinforcement Learning (IRL) is used to approximate a reward function by observing the trajectories of the system under the control of DRL-based trained controllers. The approximate reward function is then used to launch attacks by the adversary against the Deep Q Network (DQN)-based controller. Through simulation, they evaluated the effects of the two attacks under investigation and found that the attacks are increasingly successful by increasing the accuracy of the control model [11].

In their paper, Abu Khasal and Khan presented a secure industrial Internet of Things (IoT) framework for resource management in smart manufacturing. Computing-intensive tasks such as security, data analysis, decision-making, and reporting are performed in the cloud or fog using a powerful computing infrastructure. IIoT device data security is provided by improved implementation of Rivest-Shamir-Adelman (RSA)

and hash signatures. The proposed RSA algorithm has a 512-bit prime number. Device authentication is done using a hash signature. For long network lifetime, an efficient clustering method for sensor devices based on node degree (N), distance from cluster (D), residual energy (R) and fitness (NDRF) is proposed. The fitness of the sensor nodes is calculated using the Salp Swarming Algorithm (SSA). In order to reduce communication latency and overhead for IIoT devices, a resource scheduling using SoftMax Deep Neural Network (DNN) is proposed. All requests coming from the cluster head are classified using SoftMax-DNN for best resource scheduling based on storage, compute and bandwidth requirements. The proposed framework produces superior results, especially in terms of energy consumption, delay, and security strength [12].

Rozbahani et al also evaluated a snapshot set deep neural network model for attack detection in industrial Internet of Things. This paper proposes a machine learning based technique to detect cyber attacks on IIoT systems. A Snapshot Ensemble Deep Neural Network (SEDNN) is used and various metrics are evaluated including Accuracy, precision, recall and F1 score. The proposed model obtained an accuracy of 90.58% for detecting cyber attacks. Also, accuracy, recall, and F1 score were 87.42, 93.77, and 90.48%, respectively [13].

In their article, Magaya et al analyzed the industrial security of the Internet of Things with deep learning approaches for smart cities. In this paper, we present the concept of IIoT and its applications for smart cities, as well as the security challenges facing this emerging field. It then reviews the current deep learning (DL) techniques for IIoT in smart cities, which are currently mainly deep reinforcement learning, recurrent neural networks, and convolutional neural networks, and relates the advantages and disadvantages of these methods. highlights with security [14].

In the latest studies, Ting has also investigated the Internet of Things industrial intrusion detection system by neural network in the field of Internet of Things to protect the security of the privacy law. In this paper, the neural network technology for recognizing handwritten characters optimizes and improves the LeNet-5 network, and a new LeNet-7 is constructed. In addition, three network technologies are combined and an IIoT anti-intrusion detection system is built. System performance is tested and confirmed. This model has high data accuracy, detection rate and low false positive rate. The generality of the model is validated on high-performance data and compared with privacy-aware offloading methods and achieves the best performance. Therefore, this system can be applied to protect the security of data privacy law in IIoT[15].

Framework of the System

The evaluation of the use of convolutional neural network in the security of industrial Internet of Things can be summarized in several steps, which are:

1. Selection of suitable data for data mining
2. Pre-processing section
3. Presentation and construction of the model
4. Review and evaluation of the model
5. Model implementation section

6. Analysis and evaluation of results
7. Go back and start again

The general flowchart of the research includes three parts: input, processing and output. More precisely, it can be said that the inputs are the number of known attacks, the training and learning process and the pre-processing of the data, and the output is the production of a series of rules and functions that are used to detect attacks.

A. Dataset Description

In order to achieve the goals of identification and security in attacks, the following general flowchart is presented, which includes various parts of pre-processing and training with the help of convolutional neural network. In the following, each part of the flowchart is presented in detail along with the implementation details.

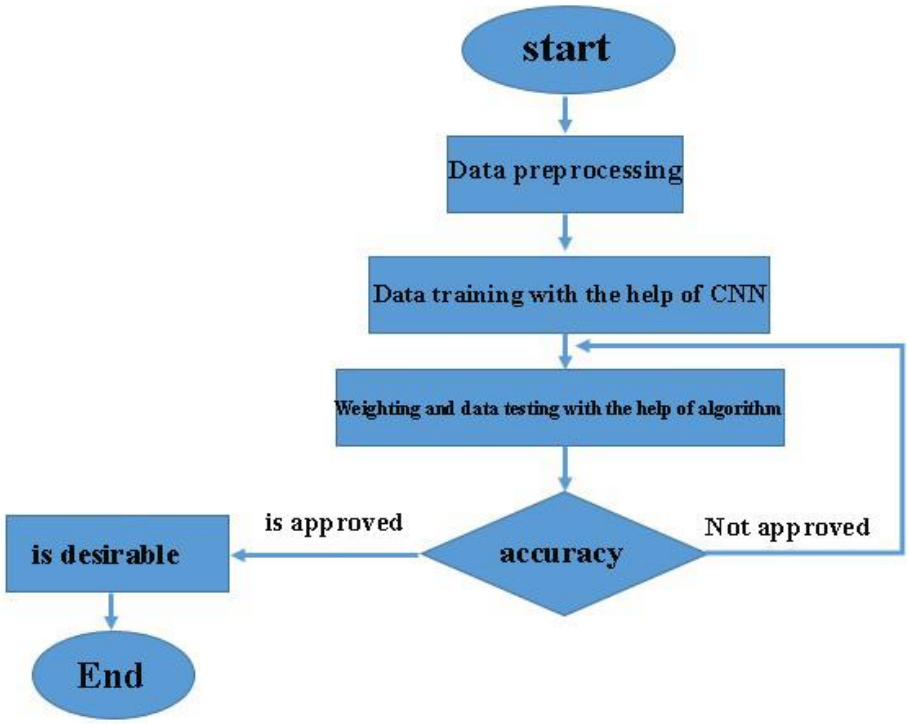

Figure 1. Flowchart of the proposed research.

B. Dataset Processing

In this research, the 99 KDD dataset is used, which contains hundreds of thousands of recorded connections. For each individual connection from Tcp/IP, different qualitative and quantitative forms were obtained. Each individual series of shapes represented an observation that was either natural or in an intrusive state. In the following, different forms are described, which were presented in reference [16].

Table 1. Description of attacks

Attacks	Description
Denial of Service (Dos)	One of the characteristics of this attack is the excessive consumption of resources, which causes rejection of normal requests to take over resources.

Probe (Scanning)	In this type of attacks, they are probed to gather information or to obtain known vulnerabilities.
Remote to local (R2L)	In this type of attack, which is called R2L, the attacker attacks the victim's machine with unauthorized and remote access, and begins to use the user's legal account to send It connects to the network.
User to Root (U2R)	These attacks are executed on the victim's machine and successfully take root.

In this research, in order to achieve the research goals and perform processing on the data, MATLAB software has been used. In the fourth chapter, the results obtained from the implementation of the algorithm in MATLAB are fully presented.

RESULTS AND DISCUSSION

Implementation and Results

Descriptive statistics, inferential statistics, as well as graphs and tables have been used to analyze the collected data. In addition, SVM, KNN and convolutional neural network algorithms were used with the optimization of weights with the help of genetic algorithm to classify and detect the attack, the results of which are also presented here.

A. Descriptive Statistics of Research Data

The results obtained in the R software and for the dataset include the median, average, standard deviation, minimum value, maximum value and standard deviation statistical indicators. The statistical information shows the data and displays all the information and characteristics that can be extracted from the data.

B. Kurtosis Descriptive Statistics

Kurtosis indicates that these data have a wide tail and a sharp tip. Here, the sharp tip of the data means that the data is better and positive, and the data tail is wide. means that the values of some data are negative.

C. Histogram Chart

By drawing the histogram of a variable, you can see the approximate shape of its distribution. In the frequency histogram, the observation of each category is specified. This function selects the number of categories automatically. This choice is such that the smoothest possible graph is also drawn while preserving partial information. This chart shows the frequency or percentage frequency of each of the classes in the form of columns. Also, by using the histogram plot and drawing the normal distribution curve, we can find out the shape of the distribution (normality, skewness and skewness) of the variable in question.

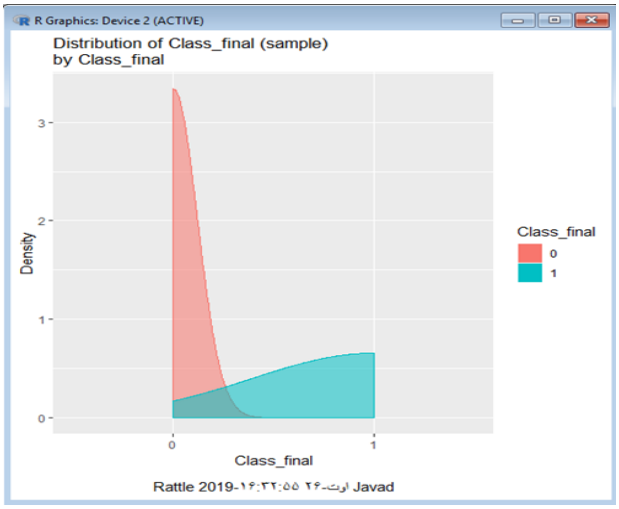

Figure 2. Normal distribution histogram of data

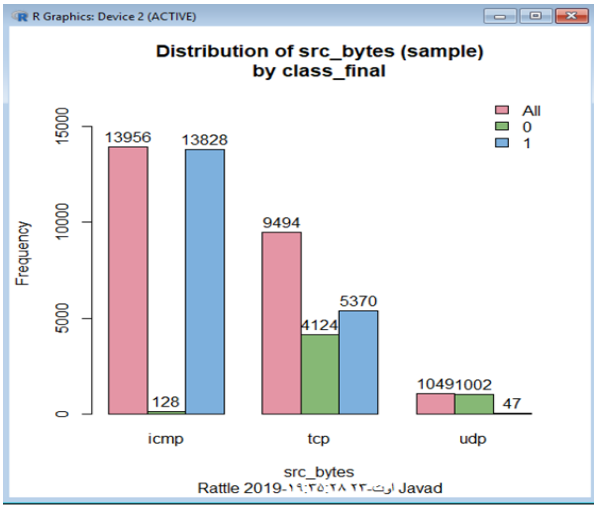

Figure 3. Barplot diagram

D. Results of KNN Algorithm

The results of odd numbers (1 to 11) for knn algorithm and 5 attacks are specified in the table below.

Table 2. Odd number results from KNN algorithm

Data Type	Normal	Probe	Dos	U2r	R2l
Dataset 1					
k-NN 1: k = 1	80. 85%	96.41%	95.77%	98. 94%	83.62%
k-NN 2: k = 3	80.84%	95. 45%	97.85%	98.83%	83.62%
k-NN 3: k = 5	75. 86%	95. 51%	93.50%	98.89%	83.47%
k-NN 4: k = 7	75. 85%	95. 69%	92.88%	98.88%	82.48%
k-NN 5: k = 9	75. 85%	95. 44%	92. 73%	98.89%	82. 50%
k-NN 6: k = 11	76. 88%	96. 74%	93. 67%	99.89%	82.55%
Dataset2					
k-NN 1: k = 1	81.85%	96. 70%	97.81%	98.72%	83.26%
k-NN 2: k = 3	80.97%	95.95%	97.74%	98.79%	83.28%
k-NN 3: k = 5	80. 96%	95.80%	97.46%	98.64%	83.24%
k-NN 4: k = 7	79. 59%	95.85%	96. 69%	98.67%	82. 14%
k-NN 5: k = 9	79. 66%	95.90%	93. 87%	98.67%	82.23%
k-NN 6: k = 11	80.80%	96.062%	92.82%	98.62%	82. 19%
Dataset3					
k-NN 1: k = 1	80.96%	96. 72%	97.88%	98.99%	83. 98%
k-NN 2: k = 3	80.73%	95.83%	97.65%	98.99%	83. 35%
k-NN 3: k = 5	81. 87%	95.79%	97. 79%	98.99%	83. 47%
k-NN 4: k = 7	75.87%	95.88%	92.93%	98.99%	82.80%
k-NN 5: k = 9	75.76%	96. 94%	92. 60%	98.99%	82.74%
k-NN 6: k = 11	75.90%	96. 70%	92. 80%	98.99%	82. 98%

Data Type	Normal	Probe	Dos	U2r	R2l
Dataset4					
k-NN 1: k = 1	81567%	96.80%	97.84%	98. 94%	83. 93%
k-NN 2: k = 3	80.2003%	95.64%	96.28%	98.63%	83.93%
k-NN 3: k = 5	78.9667%	95.70%	95.35%	98. 93%	83. 74%
k-NN 4: k = 7	75.7613%	95.76%	92.74%	98. 93%	82.83%
k-NN 5: k = 9	75.7551%	95.93%	92.50%	98.89%	82.83%
k-NN 6: k = 11	75.7999%	96. 74%	92. 71%	98.89%	82.81%
Dataset5					
k-NN 1: k = 1	81. 60%	96.86%	97.78%	98. 51%	83. 41%
k-NN 2: k = 3	76.35%	95.99%	93. 54%	98. 62%	83.37%
k-NN 3: k = 5	76. 26%	95.70%	93. 68%	98.75%	83. 38%
k-NN 4: k = 7	76.09%	95.86%	92. 77%	98.60%	82.80%
k-NN 5: k = 9	76.35%	95.95%	92.63%	98. 84%	82.74%
k-NN 6: k = 11	76.28%	96.16%	92.61%	98.60%	82.73%

E. Results of Neural Network Training and optimization

The results obtained from the genetic algorithm for 5 attacks in this research and in 100 repetitions have been obtained in the following forms.

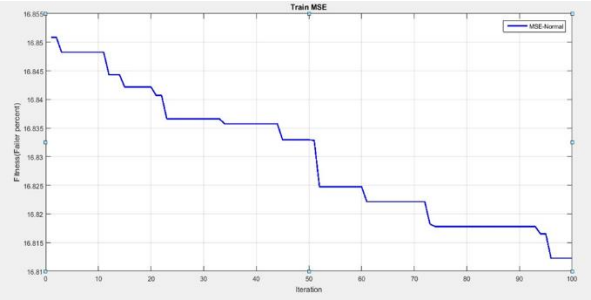

Figure 4. Optimization results for Normal attack

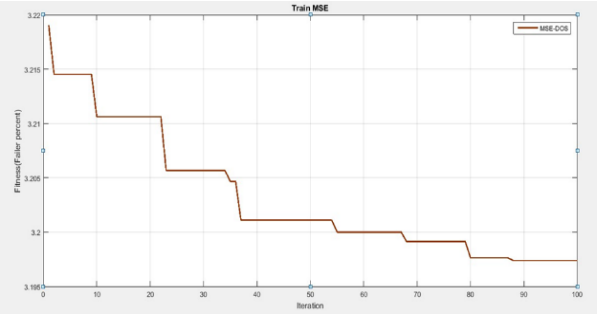

Figure 5. Optimization results for DOS attack

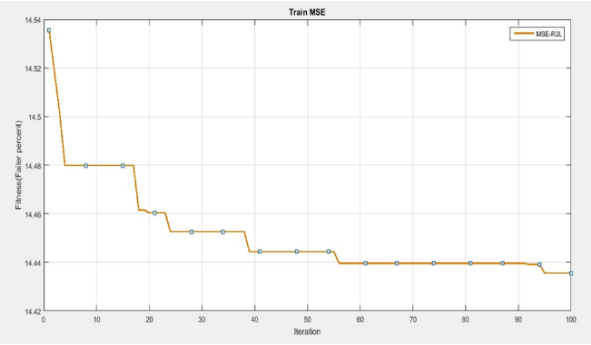

Figure 6. Optimization results for R2L attack

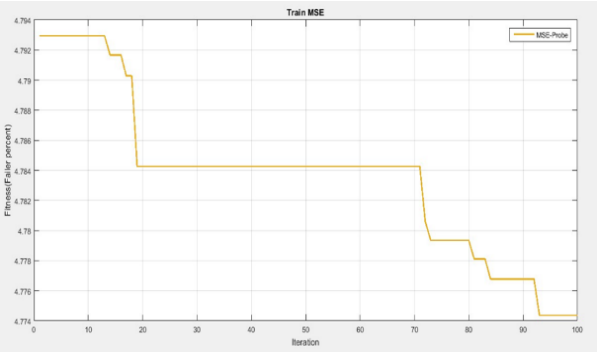

Figure 7. Optimization results for Probe attack

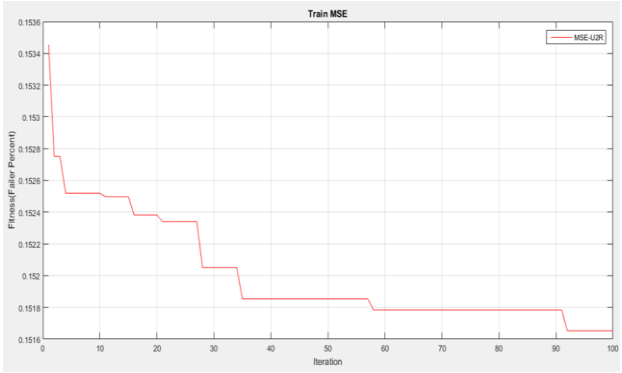

Figure 8. Optimization results for U2R attack

The following table shows the results obtained from convolutional neural network training and optimization of training weights in order to increase accuracy in detecting attacks. As you can see, the U2R attack has an excellent result of 99.85. The mentioned algorithm has been 96.8% successful in DOS and Probe attacks. But the results for R2L and Normal attacks are 85.6 and 83.2 respectively. Which is not great but the results are decent.

Table 3. Summary of the results

Genetic algorithm detection percentage	Amount of GA algorithm training errors	Type of attack
83.2 %	16.8 %	Normal
96.8 %	4.7 %	Probe
96.8 %	3.2 %	Dos
99.85 %	0.15 %	U2R
85.6 %	14.4 %	R2L

F. Comparison of SVM, KNN and CNN Algorithms

SVM, KNN or neural network based algorithms have been used in many articles. The important point is that each article is focused on one or a number of attacks, and on the other hand, their data or datasets are also different, but the number of data plays a very decisive role in education. Therefore, comparing our results with other articles is not completely correct due to the wide range of parameters, but in this thesis, in order to compare learning algorithms in attack detection, 5 attacks were considered and SVM, KNN and Convolutional Neural Network algorithms were used with a single dataset. was made so that the comparison of the results is reliable. Therefore, the following table shows the results of success in attack detection for all three algorithms.

Table 4. Comparison of the results of all three SVM, KNN and CNN algorithms

Convolutional neural network	KNN	SVM	Type of attack
83.2 %	81.87 %	76.91 %	Normal
96.8 %	96.94%	96.75 %	Probe
96.8 %	97.84 %	99.97 %	Dos

99.85 %	98.99 %	84.8 %	U2R
85.6 %	83.98 %	83.92 %	R2L

CONCLUSION

Fundamental Finding : Today, intrusion detection systems based on data mining have been proposed. Identifying patterns in large amounts of data helps us a lot. Data mining methods can detect abnormal data by specifying a binary label (normal packet, abnormal packet) and also specifying the features and characteristics with classification algorithms. Therefore, the accuracy and correctness of intrusion detection systems is increased and as a result, network security is increased. There are different methods and algorithms for data mining, in this research, machine learning, neural network, and optimization of weights with the help of genetic algorithm were used. In machine learning, combinations of classifiers, known as ensemble classifiers, often outperform individuals. While there are many group approaches, finding the right group configuration for a particular data set is difficult. In this research, a new grouping method is presented, which uses the generated genetic weights to create a set of classifications with better detection of permeability. The obtained results showed that the convolutional neural network is more accurate in detecting 5 attacks than SVM and KNN algorithms, and it can be used in the security sector of industrial Internet of Things. **Implication :** The findings imply that using genetic algorithm-based optimization of neural network weights can significantly enhance the detection accuracy of intrusion detection systems, especially when applied to industrial Internet of Things environments. The convolutional neural network demonstrated higher accuracy in identifying multiple attack types, indicating its potential application in real-time network security monitoring. This result suggests that machine learning-based intrusion detection systems can play a crucial role in enhancing cybersecurity and protecting industrial infrastructures from cyberattacks. **Limitation :** The data set used is a very complete data set, and in this project, about 350,000 data were used as training and testing data for the neural network, however, the obtained findings were acceptable, but it is suggested that the percentage increase success in other studies. More data should be used in neural network training. Although the CNN achieved promising accuracy, the study was conducted in a simulation environment using the KDD99 dataset, which may not fully reflect the complexity of modern industrial IoT traffic patterns. **Future Research :** According to the findings obtained from the proposed design used in this research, it is suggested to use other optimization designs in the body of the neural network in future studies in order to increase the speed of convergence of the results, as well as the possibility of increasing the accuracy of detecting the existence of it. It is also recommended that future studies expand the size and diversity of the dataset to improve the generalization ability of the model. According to the findings, it seems that this method can be used for the industrial Internet of Things, but it needs confirmation and more work. Therefore, it is recommended to implement and test it in the form of hardware in the next studies.

REFERENCES

[1] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, "Multimedia Internet of Things: A comprehensive survey," *IEEE Access*, vol. 8, pp. 8202–8250, 2020.

[2] R. Qaddoura and S. Manaseer, "Comparative Study for the Effect of CPU Speed in Fog Networks," in *Proc. 5th Int. Symp. Innovation Inf. Commun. Technol. (ISIICT)*, Amman, Jordan, Oct. 31–Nov. 1, 2018, pp. 1–5.

[3] T. Alam, "Internet of Things: A Secure Cloud-based MANET Mobility Model," *Int. J. Netw. Secur.*, vol. 22, pp. 514–520, 2020.

[4] C. Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, and G. Fortino, "Agent-based Internet of Things: State-of-the-art and research challenges," *Future Gener. Comput. Syst.*, vol. 102, pp. 1038–1053, 2020.

[5] N. Angelova, G. Kiryakova, and L. Yordanova, "The great impact of Internet of Things on business," *Trakia J. Sci.*, vol. 15, pp. 406–412, 2017.

[6] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the Internet of Things," *Sensors*, vol. 19, p. 1977, 2019.

[7] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in *Proc. IEEE Int. Conf. Intelligence and Security Informatics (ISI)*, Beijing, China, Jul. 22–24, 2017, pp. 179–181.

[8] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms," *Future Internet*, vol. 15, no. 6, Jun. 2023. IDEAS/RePEc+1

[9] S. Nandhini, A. Rajeswari, and N. R. Shanker, "Cyber attack detection in IoT-WSN devices with threat intelligence using hidden and connected layer based architectures," *Journal of Cloud Computing*, vol. 13, Art. no. 159, 2024.

[10] C. S. Kumar, "Correlating Internet of Things," *Int. J. Manage.*, vol. 8, pp. 68–76, 2017.

[11] L. Columbus, "Roundup of Internet of Things forecasts and market estimates, 2016," *Forbes*, 2016. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016

[12] L. Dignan, "IoT devices to generate 79.4 ZB of data in 2025, says IDC," *ZDNet*, 2019. [Online]. Available: https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc

[13] J. R. A. Gerber, "Connecting all the things in the Internet of Things," IBM Developer, 2020. [Online]. Available: https://developer.ibm.com/technologies/iot/articles/iot-lp101-connectivity-network-protocols/

[14] Internet of Things World Forum (IoTWF), "IoTWF leaders announce new IoT reference model and IoTWF talent consortium," 2014. [Online]. Available: https://telecomreseller.com/2014/10/14/internet-of-things-world-forum-iotwf-leaders-announce-new-iot-reference-model-and-iotwf-talent-consortium/

[15] S. Farahani, "Zigbee and IEEE 802.15.4 protocol layers," in *ZigBee Wireless Networks and Transceivers*, Burlington, MA: Newnes, 2008, pp. 33–135. doi: 10.1016/B978-0-7506-8393-7.00003-0.

[16] V. Stoffer, "Outdated computers and operating systems," 2013. [Online]. Available: https://commons.lbl.gov/display/cpp/Outdated+Computers+and+Operating+Systems

*Nameer Majid Hashim (Corresponding Author) 10pt
Independence Researcher
Email: nnameer7@gmail.com