International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 3, June 2023, pp. 3072~3078
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i3.pp3072-3078

Detecting network attacks model based on a convolutional neural network

Teba Ali Jasim Ali, Muna M. Taher Jawhar
Software Department, College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq

Article Info

Article history:

Received May 25, 2022
Revised Sep 28, 2022
Accepted Dec 2, 2022

Keywords:

Convolutional neural network
CSE-CIC-IDS2018
Deep learning
Network security

ABSTRACT

Due to the increasing use of networks at present, Internet systems have raised many security problems, and statistics indicate that the rate of attacks or intrusions has increased excessively annually, and in the event of any malicious attack on network vulnerabilities or information systems, it may lead to serious disasters, violating policies on network security, i.e., "confidentiality, integrity, and availability" (CIA). Therefore, many detection systems, such as the intrusion detection system, appeared. In this paper, we built a system that detects network attacks using the latest machine learning algorithms and a convolutional neural network based on a dataset of the CSE-CIC-IDS2018. It is a recent dataset that contains a set of common and recent attacks. The detection rate is 99.7%, distinguishing between aggressive attacks and natural assertiveness.

Corresponding Author:

Muna M. Taher Jawhar
Software Department, College of Computer Sciences and Mathematics, University of Mosul
Mosul, Iraq
Email: dr.muna_taher@uomosul.edu.iq

1. INTRODUCTION

Nowadays, the internet of things (IoT) devices have increased as well as the data generated by these devices, and a lot of basic activities are carried out by the network, so the network is considered one of the essential parts of life [1], and this has led to an increase in the incentive to attack the network and information systems. Therefore, it becomes difficult for normal traditional detection tools to deal with these attacks efficiently [2] due to the multiple constraints that the network constantly imposes on the network and IoT devices. An effective and lightweight system that detects attacks on the network is required to detect cyber anomalies. It classifies various electronic attacks. To address this problem requires creating a predictive model that detects or predicts attacks on a network. Intrusion detection is the act of dynamically monitoring and analyzing events that occur on a computer system or network in order to detect possible assaults and prevent unwanted access. This is often done by automatically gathering data from a range of network sources.

Then it evaluates the data for security flaws. Therefore, network attack detection systems are an essential information security tool. When an attack or violation is identified in network traffic, attack detection systems generate an alert to warn the user that an attack has happened so that necessary action may be taken. network intrusion detection systems (NIDS), in conjunction with other traditional security measures such as firewalls, access control systems, and antivirus software, are used to safeguard network information and communications systems against assaults. Due to the increase in the number of attacks and advanced threats, traditional intrusion detection systems cannot keep up. They have faults, necessitating the development of a strong attack detection system [3], especially now that machine learning has become a prominent way of identifying sophisticated assaults with unexpected patterns based on algorithms. Statistical and mathematical algorithms, rather than rule-based algorithms machine learning approaches help to improve the performance

of intrusion detection system (IDS), so we relied in this research on machine learning techniques to build a detection model using convolutional neural network (CNN) [4].

Many researchers have built models to detect attacks that threaten networks in general and the IoT in particular. Ahmad *et al.* [5] created an intrusion detection system based on CNN using the CIC-2018 dataset, which they converted into images before organizing convolutional layers and max-pooling layers for CNN. Tamy *et al.* [6] built a model based on deep learning for detecting cyber-attacks based on the database CIC-2018. The detection rate was good, close to 90%. Niyaz *et al.* [7] designed a system that analyzes network traffic data and detects cyber-attacks based on neural networks. The accuracy rate was 99.97%, and the false positive rate was 0.03 for detected botnet attack classification. Dang *et al.* [8] designed an intrusion detection system based on the network simulation knowledge discovery and data mining (NSL-KDD) dataset by using CNN. The detection ratio of the system was 83.31%. Mohammed *et al.* [9] built a model based on the CNN network with three designs that differ in terms of the number of layers and the size of the windows adopted in the first layers with the use of two types of data: NSL-KDD and UNSWNB15. Yin *et al.* [10] proposed a model for intrusion detection based on neural networks of type recurrent neural networks (RNN). The model was built on forward propagation and backward propagation and used with NSL-KDD data and the detection results for binary classification was 83.28% while for multiclass classification it was 81.29%. Furthermore, we may be able to increase performance in the future by utilizing these sophisticated models. Chandre *et al.* [11] proposed a deep learning algorithm in the intrusion detection system for wireless networks using wireless sensor network data set (WSNDS). The results obtained showed an accuracy of 97%. A deep learning long-term memory (LSTM) algorithm was used in [12] to analyze the dataset of "CSE-CIC-IDS2018" network traffic, which analyzes network traffic for normal behavior and attacks. It regularly achieved a detection accuracy of 99%. Farhan *et al.* [13] used a deep learning algorithm deep neural network (DNN) to test intrusion detection on the "CSE-CIC-IDS2018" dataset containing hundreds of packets of real network traffic, and an attack detection accuracy of about 90% was obtained. Ramasamy and Eric [14] developed a deep packing-based convolutional neural network (DBCNN) for intrusion detection networks in the tested KDD dataset where the accuracy they obtained was 99%. The rest of this paper is structured as. Section 2 provides a brief overview of the CIC2018 dataset. In section 3, we describe our approach, which uses CNN to identify threats. Section 4 discusses the methodology of the model. Section 5 experimental results in our model. Finally, section 6 has its conclusion.

2. THE DATASET

There are many famous databases that are approved by most researchers, such as the dataset CSE-CIC-IDS2018. It was created through cooperation between the Communications Security Corporation (CSE) and the Canadian Cyber Security Institute (CIC). Due to changing network behaviors and patterns and the evolution of attacks on the internet, it has become vital to transition away from static data sets and toward dynamically produced data sets that are adjustable, expandable, and repeatable [15]. It is the latest data set to detect intrusions or attacks on network traffic. Its huge data contains a wide range of attack types in addition to the benign type. The CIC-IDS2018 dataset contains seven types of attacks. Botnets, Heartbleed, brute force, denial of service and dis-attributed denial of service, inside network penetration, and web assaults are among the 80 characteristics retrieved from traffic recorded with CICFlowMeter-V3 [16].

3. CONVOLUTIONAL NEURAL NETWORK

Deep learning is a powerful way to make accurate predictions from large datasets such as images, text, or videos. Deep learning capabilities, which have multiple processing layers, make it possible to learn blurred and hidden representations of data. The characteristics of deep learning have been taken advantage of in the field of cyber security [17]. Especially in the classification and detection of malware, it saves a lot of time and enhances the accuracy of the whole malware detection system. Modern deep learning technologies, introduced in the realm of cyber security and especially attack detection, have outperformed traditional machine learning methods due to their ability to extract features automatically in a hierarchical manner rather than engineering the features into machine learning [18]. Furthermore, the usual feature extraction approach is not directly employed to categorize the error mode. Therefore, a model that achieves the co-optimization of feature extraction and pattern recognition provides deep learning, as shown in Figure 1, shows how to select features and extract features in machine learning and deep learning [19].

To realize this idea, a CNN was used, a deep learning structure [3], [20], also called a ConvNet, which is a modification of the traditional feed-forward neural network. CNN was inspired by the mammalian visual cortex and has since become the industry standard for data analysis [21]. It is made up of several convolutional and aggregation layers that work together to perform feature extraction and data scaling reduction. The fully linked layer is then used to categorize the output layer and output the results [22], [23]. The deep learning algorithm CNN has achieved many successes in solving computer task problems such as classification, object

detection, and pattern recognition, as well as success in reducing data dimensions in a way that is easy to process without losing the necessary features to access. The exquisite performance of the model, according to deep learning models, is the structure of a well-trained CNN model, as shown in Figure 2 [24], [25].

CNNs are one of the finest learning algorithms for comprehending complicated structures, and they have demonstrated exceptional performance in picture segmentation, object identification, and computer vision applications. The fundamental benefit of CNNs is their capacity to exploit spatial or temporal correlations in data. CNNs have also been utilized for feature extraction and categorization in the context of attack detection. The CNNs reduce the complexity of the model during its phases, and thus the learning process is improved compared to other deep learning architectures [26], [27].

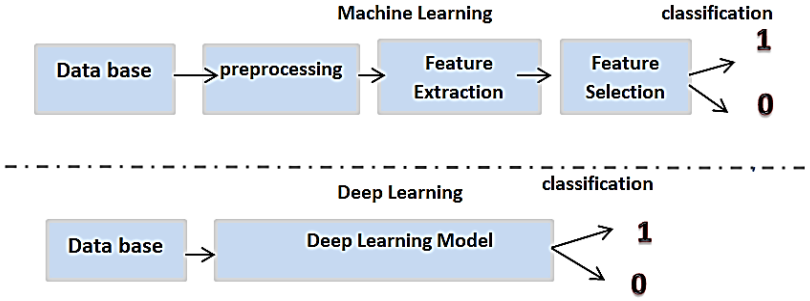


Figure 1. Comparison of deep learning and machine learning when extracting feature

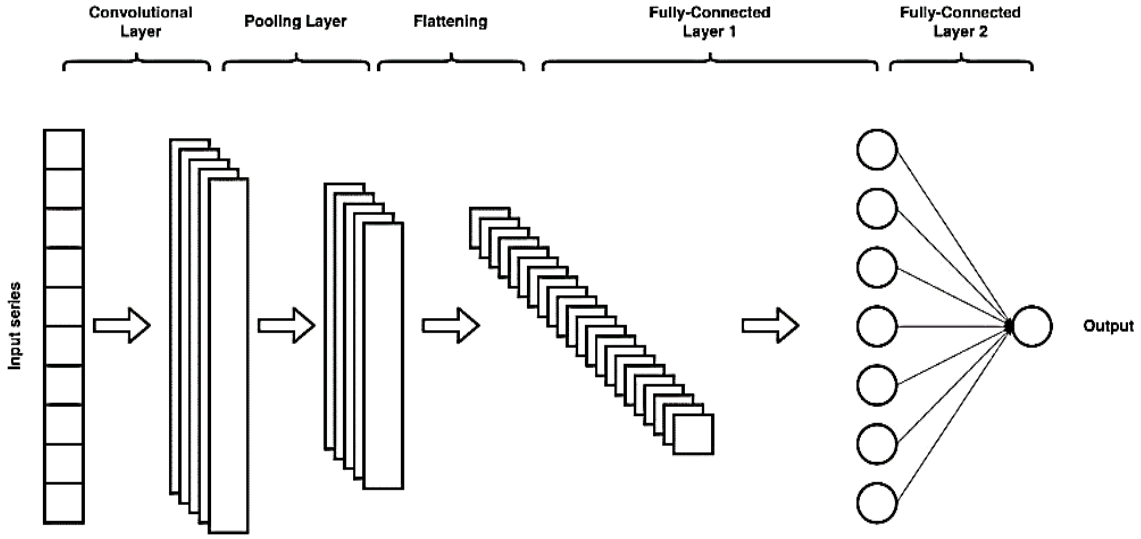


Figure 2. The CNN architecture and fully connected layers

4. METHOD

The first step we took in this research was to process the data due to its large size and consisting of some missing and redundant data records. These problems can therefore be addressed by preprocessing (feature engineering) of the data samples or by eliminating missing records. Then, we preprocess the data set to be suitable for applying machine learning techniques according to the following steps.

a) After being addressed by the CSE-CIC-IDS2018 dataset, we process missing and infinity data in two ways. The first method removes all missing and infinite values. The second method replaces the data sets with infinite values with the maximum value and the missing values with the average values.
b) The process of picking some features from data and eliminating the unnecessary ones is known as feature selection. Therefore, we did some categorical features. These categorical features led to an increase in the training time of the network.
c) Categorical data encryption.
d) Divide the data set into a training set and a test set.

e) Normalize the data set: The numerical data in the data set contains different ranges, as a result the classification model will face some challenges during training to compensate for these differences. The minimum in each attribute is zero, and the maximum is one. Thus, we will get homogeneous values for the classifier while maintaining the relativity between all the attributes. After formatting the data, reducing dimensionality, and dropping unnecessary features that improve the ability to classify, we notice that the data set consists only of numeric values that do not have or need a spatial relationship with each other, the embedding layer can be dropped, and the data can be transferred directly to our neural network as shown in Figure 3. At this point, there are many ways to build a model. Here is a simple model.

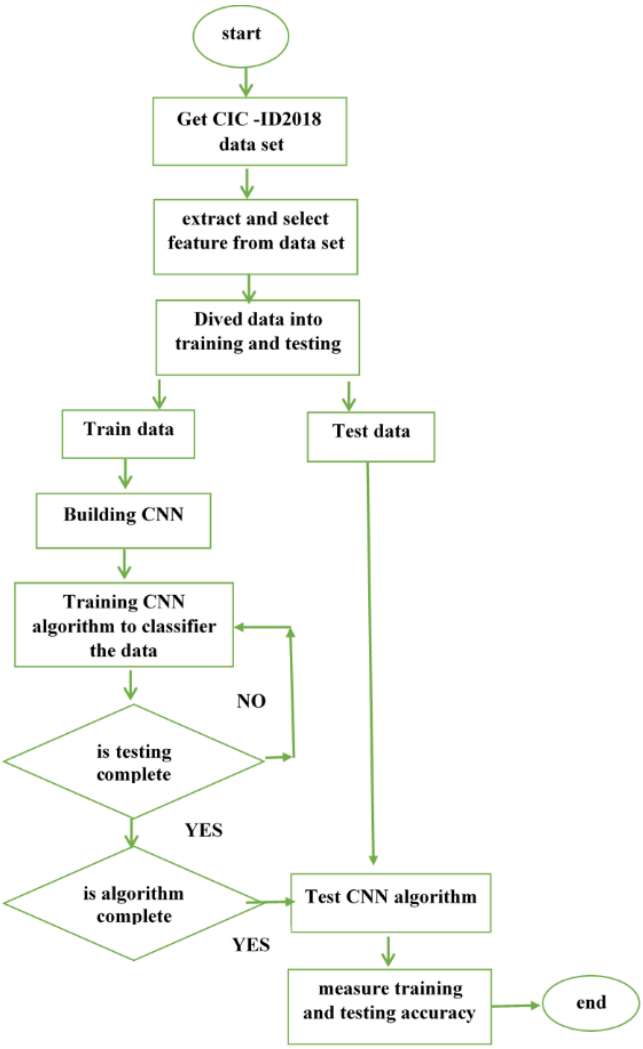


Figure 3. The algorithm of the proposed model

We used a one-dimensional CNN model with training data (80% of the data) and foundation libraries including Keras, Pandas, NumPy, and Scikit-learn. The three layers of our sequential CNN model consist of a convolutional layer with 64 nodes and kernels of size 3, an activation function called ReLU that is applied to each numerical value and replaces all negative values in the features with zero, and a layer called maxpooling that is positioned behind the convolutional layer. Although the max pooling layer is not necessary for a CNN model, we nevertheless use it because, because the translated input only contains numerical information, there is very little possibility that we will lose important features as a result of the max pooling. Additionally, a flatten layer is put before a dense layer and a dropout with a rate of 0.25. Being near the end of the network means that every time a process involves the random selection of 75% of the nodes, it will increase the unpredictability of the model and decrease bias. Figure 4 depicts a CNN design with one convolutional layer, one pooling layer that generates the maximum value of two neighboring elements, two fully connected layers, an input layer followed by a dropout layer, and an output layer as its last layer.

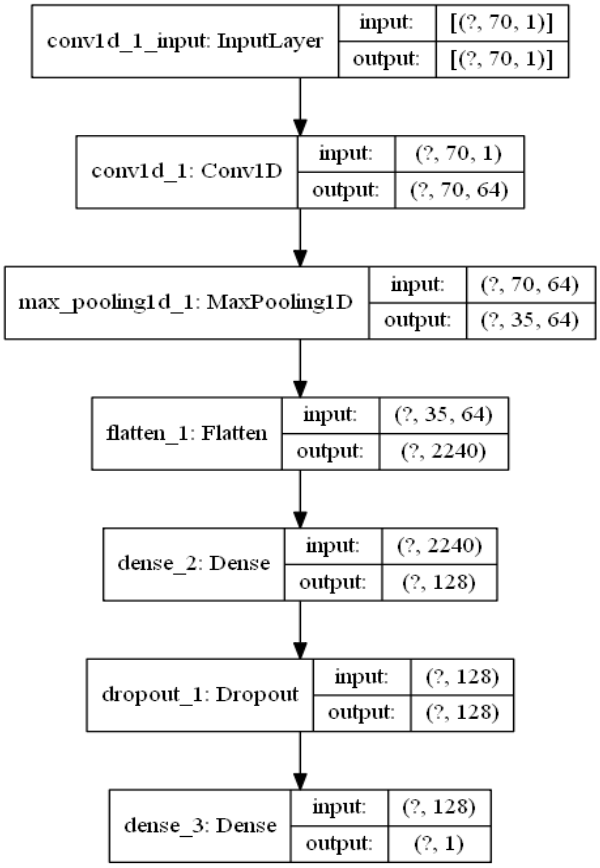
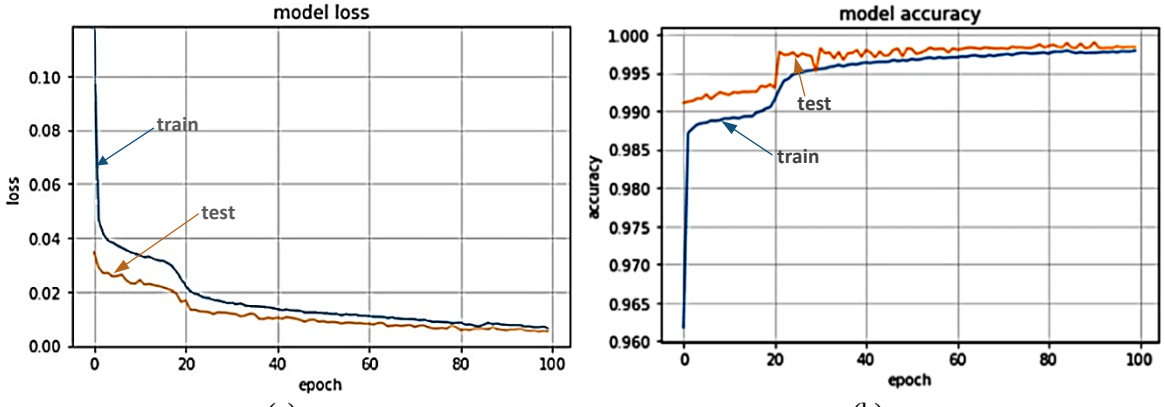


Figure 4. Block diagram of CNN model

5. RESULTS AND DISCUSSION

For our model, the "ADAM" optimizer was used with batch size=128, epoch=100. While the activation function was "Sigmoid" for the output layer. Their summaries are given in Table 1. The tested model was initially used with a test dataset, and after that, as shown in Figures 5, Figure 5(a) show the loss ratio of the model and Figure 5(b) show accuracy, it underwent accuracy analysis and performance evaluation, better detection rates, attack type classification, and connection type classification to determine whether a connection is normal or problematic. It successfully distinguished between offensive and common contact with an accuracy rate of 99.7%. We compared our model with the previous researcher's models; Table 2 illustrates the result of another research with our model.



(a) (b)

Figure 5. Curve of (a) loss and (b) accuracy

Table 1. Parameters used in our mode

Model: sequential		
Layer (type)	Output shape	Param #
Conv1d(conv1D)	(None, 70, 64)	256
Max_pooling1d (Maxpooling1D)	(None, 35, 64)	0
Flatten(flatten)	(None, 2240)	0
Dense (dense)	(None, 128)	286848
Dropout (dropout)	(None, 128)	0
Dense_1 (dense)"	(None, 1)	129

Table 2. Comparison with another research

Reference	Method	Dataset	Detection rate %	Year
Yin *et al.* [10]	RNN	NSL-KDD	83.28	2017
Liu *et al.* [23]	CNN	NSL-KDD	83.31	2018
Maithem and Al-sultany [3]	CNN	NSL-KDD	88.81	2021
		UNSWNB15	90.25	
Farhan *et al.* [13]	DNN	CSE-2018	90	2020
Chandre *et al.* [11]	Deep learning	WSNDS	97	2022
Farhan *et al.* [12]	LSTM	CSE-2018	99	2022
Our model	CNN	CIC- 2018	99.7	2022

6. CONCLUSION

Detection of attacks is the process of monitoring and analyzing events that occur in network traffic to obtain indications of attacks or intrusions on the network. Because most of the techniques used today are not able to deal with the dynamic nature of attacks on networks. Hence, adaptive and dynamic approaches such as machine learning techniques can lead to higher discovery rates, lower computational costs, and reasonable communication. Therefore, intrusion detection systems are very important tools for protecting information and limiting the damage caused by attacks on information and network security.

In our research, we built a system that detects network attacks using CNN, based on a set of the CSE-CIC-IDS2018 standard data widely used by many researchers. It is a recent dataset that contains a set of common and recent attacks. The program underwent training and testing. Using the Python language and the Jupiter Notebooks code editor, classification accuracy, detection rates, and error rates were evaluated. The outcomes of real-world tests reveal enhanced efficiency when applied. It is preferable to use the low-attribute dataset as opposed to the full-attribute dataset, which has improved detection rates and classification of types of attacks and enables the type of connection to be normal or abnormal. It reached an accuracy rate of 99.7%.

REFERENCES

[1] C. Wu and W. Li, "Enhancing intrusion detection with feature selection and neural network," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3087–3105, Jul. 2021, doi: 10.1002/int.22397.

[2] R. Marwaha, "Intrusion detection system using data mining techniques– A review," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 5, pp. 450–452, May 2017, doi: 10.23956/ijarcsse/V7I5/0161.

[3] M. Maithem and G. A. Al-sultany, "Network intrusion detection system using deep neural networks," *Journal of Physics: Conference Series*, vol. 1804, no. 1, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012138.

[4] I. Benmessahel, K. Xie, and M. Chellal, "A new evolutionary neural networks based on intrusion detection systems using multiverse optimization," *Applied Intelligence*, vol. 48, no. 8, pp. 2315–2327, Aug. 2018, doi: 10.1007/s10489-017-1085-y.

[5] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.

[6] S. Tamy, H. Belhadaoui, M. A. Rabbah, N. Rabbah, and M. Rifi, "Select the best machine learning algorithms for prediction and classification of intrusions using KDD99 intrusion detection dataset," *Indian Journal of Science and Technology*, vol. 12, no. 37, pp. 1–6, Oct. 2019, doi: 10.17485/ijst/2019/v12i37/147551.

[7] Q. Niyaz, W. Sun, and A. Y. Javaid, "A deep learning based DDoS detection system in software-defined networking (SDN)," *ICST Transactions on Security and Safety*, vol. 4, no. 12, Dec. 2017, doi: 10.4108/eai.28-12-2017.153515.

[8] V. T. Dang, T. T. Huong, N. H. Thanh, P. N. Nam, N. N. Thanh, and A. Marshall, "SDN-based SYN proxy—A solution to enhance performance of attack mitigation under TCP SYN flood," *The Computer Journal*, vol. 62, no. 4, pp. 518–534, Apr. 2019, doi: 10.1093/comjnl/bxy117.

[9] J. Mohammed, M. Hussain, and U. Mirza, "Brachial plexus injury: Following birthday bumps," *Journal of Orthopaedics and Allied Sciences*, vol. 6, no. 2, 2018, doi: 10.4103/joas.joas_23_18.

[10] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[11] P. R. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 11, no. 2, pp. 504–515, Jun. 2022, doi: 10.11591/ijai.v11.i2.pp504-515.

[12] B. I. Farhan and A. D. Jasim, "Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 26, no. 2, pp. 1165–1172, May 2022, doi: 10.11591/ijeecs.v26.i2.pp1165-1172.

[13] R. I. Farhan, A. T. Maolood, and N. F. Hassan, "Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 20, no. 3, pp. 1413–1418, Dec. 2020, doi: 10.11591/ijeecs.v20.i3.pp1413-1418.
[14] M. Ramasamy and P. V. Eric, "An improved deep bagging convolutional neural network classifier for efficient intrusion detection system," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 405–413, 2022, doi: 10.11591/eei.v11i13252.
[15] Z. Cui, F. Xue, X. Cai, Y. Cao, G. Wang, and J. Chen, "Detection of malicious code variants based on deep learning," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3187–3196, Jul. 2018, doi: 10.1109/TII.2018.2822680.
[16] A. Midzic, Z. Avdagic, and S. Omanovic, "Intrusion detection system modeling based on learning from network traffic data," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 11, pp. 5568–5587, Nov. 2018, doi: 10.3837/tiis.2018.11.022.
[17] H. G. Kayacık, A. N. Zincir-Heywood, and M. I. Heywood, "Selecting features for intrusion detection a feature relevance analysis on KDD 99 intrusion detection datasets," in *Conference on Privacy, Security and Trust. The Fairmont Algonquin*, 2005, pp. 1–6.
[18] L. Dhanabal and S. P. Shantharajah, "A study of NSL-KDD dataset for intrusion detection system based on classification algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446–452, 2015, doi: 10.17148/IJARCCE.2015.4696.
[19] S. El-Sappagh, A. S. Mohammed, and T. A. AlSheshtawy, "Classification procedures for intrusion detection based on KDD cup 99 data set," *International Journal of Network Security & Its Applications*, vol. 11, no. 03, pp. 21–29, May 2019, doi: 10.5121/ijnsa.2019.11302.
[20] Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 8, pp. 1798–1828, Aug. 2013, doi: 10.1109/TPAMI.2013.50.
[21] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, Apr. 2015, doi: 10.1016/j.eswa.2014.11.009.
[22] J. Heaton, "Ian goodfellow, yoshua bengio, and aaron courville: Deep learning," *Genetic Programming and Evolvable Machines*, vol. 19, no. 1–2, pp. 305–307, Jun. 2018, doi: 10.1007/s10710-017-9314-z.
[23] Y. Liu, S. Liu, and Xi. Zhao, "Intrusion detection algorithm based on convolutional neural network," *DEStech Transactions on Engineering and Technology Research*, Mar. 2018, doi: 10.12783/dtetr/iceta2017/19916.
[24] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, May 2017, doi: 10.1145/3065386.
[25] D. Roy, P. Panda, and K. Roy, "Tree-CNN: A hierarchical deep convolutional neural network for incremental learning," *Neural Networks*, vol. 121, pp. 148–160, Jan. 2020, doi: 10.1016/j.neunet.2019.09.010.
[26] A. Mahendran and A. Vedaldi, "Visualizing deep convolutional neural networks using natural pre-images," *International Journal of Computer Vision*, vol. 120, no. 3, pp. 233–255, Dec. 2016, doi: 10.1007/s11263-016-0911-8.
[27] R. Singh and G. Srivastav, "Novel framework for anomaly detection using machine learning technique on CIC-IDS2017 dataset," in *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, Nov. 2021, pp. 632–636. doi: 10.1109/ICTAI53825.2021.9673238.

BIOGRAPHIES OF AUTHORS

Teba Ali Jasim Ali is a master's student in the Software Department, College of Computer Science and Mathematics, Mosul University. Her specialized areas of research are software engineering, and smart technologies. Her profile can be found at https://www.researchgate.net/profile/Tyba-A-Jasim and she can be contacted at email: tebaa.20csp6@student.uomosul.edu.iq.

Muna M. Taher Jawhar is an instructor in the Software Department, College of Computer Science and Mathematics, Mosul University. She holds a Ph.D. in computer science. Her specialized areas of research are network security, intelligence, and confidentiality techniques. She can be contacted at dr.muna_taher@uomosul.edu.iq.