Computational Sciences and Engineering 3(2) (2023) 253-263

University of Guilan

Computational Sciences and Engineering

journal homepage: https://cse.guilan.ac.ir/

Anomaly Detection System in the Industrial Internet of Things Network with Convolutional Neural Network

Rahim Asghari [a,*], Sajjad Ghasemzadeh [b], Mohammad Allahyari [c]

[a] Department of mathematics, Technical and Vocational University, Tehran, Iran
[b] University of Tehran, College of Engineering, Tehran, Iran
[c] Urmia University of Technology, Urmia, Iran

ARTICLE INFO

Article history:
Received 17 November 2023
Received in revised form 29 December 2023
Accepted 13 February 2024
Available online 13 February 2024

Keywords:
Industrial internet of things
Network security
Intrusion detection system
Deep learning
Convolutional neural network.

ABSTRACT

Today, information security and preventing data theft are of great importance in the industrial Internet of Things. For this reason, in order to improve the network, it is necessary to use a suitable intrusion detection system to detect anomalies and improve the network. Machine learning is one of the powerful methods used for network modeling and diagnosis. In this article, with the help of convolutional neural network modeling, which is considered one of the powerful methods of machine learning, an intrusion detection system with optimal performance in abnormal traffic detection is presented. In this method, the proposed model is implemented and shown in several classes. Also, data processing to NSL-KDD datasets is applied in this paper to obtain appropriate results that indicate the appropriate quality of the proposed evaluation model; Therefore, according to the simulation results, the accuracy and true positive rate of the NSL-KDD data set, and the proposed neural network model, the accuracy and true positive rate on the NSL-KDD data set have reached 92.3% and 88.5%, respectively.

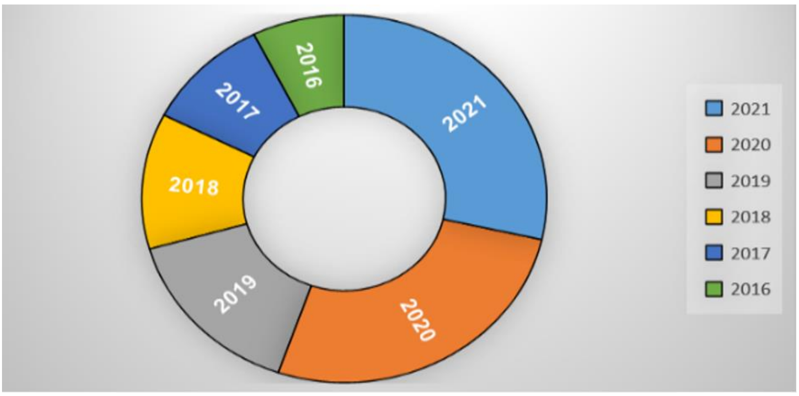
1. Introduction

Attacks on computer networks have greatly increased with the growth of these networks. to deal with these attackers in computer networks and systems, several methods known as intrusion detection techniques have been developed. intrusion refers to any unauthorized act that endangers confidentiality or availability of a resource. the purpose of the Process is to identify intrusion detection intrusion, misuse and possible damage to computer systems and networks. The distinction is more difficult to detect in recent years. The influence is usually made using the destructive software of worms, viruses, police, and spies. Hanks usually watch the to steal private information

[*] Corresponding author.
E-mail addresses: rasghari@tuv.ac.ir (R. Asghari)

https://doi.org/10.22124/cse.2024.26046.1069

and hurt someone else. The diagnostic system controls the network's communications to look for destructive activity. The recognition of a major challenge for security experts in the cyber world. Many types of the immune system have demonstrated an excellent performance using machines to identify their attacks. however , their limitations in terms of data cause complexity in deep learning methods .as a result , it is stated that with the advancement of technology , the number of people connecting the internet is rapidly increasing .by april 2022 , there are five billion internet users worldwide, 63 percent of the world's population [1] .another part called intrusion prevention systems, which detect intrusion detection systems in their core , detects intrusion detection system in fact only the entry of illegal individuals to the network , but intrusion prevention systems prevent illegal access to the network .intrusion detection system analyzes network packets , when the intrusion is detected , the alarm clock is generated for the offending packets or interruption . The evolution in different fields of technology, such as sensors and automotive identity, automatic calculations, cordless communications, internet access to the wide, and distribution services, has caused potential to increase the integrity of all living things on the internet. The 'Erb' is a compliment to the intelligence of things being connected with one another This example of the new model is known as one of the most important factors in the field of information and communication technology for the coming years. According to the prediction of Gar Internet of Things company, it may reach 26 million units by 2020. Also, Cisco systems have predicted that the Internet of Things will reach the amount of 14.4 trillion between the years 2013 and 2020 in the combination of increasing revenues and reducing the costs of companies. Intrusion detection systems are among the tools that are used to protect networks and industrial information systems. The intrusion detection system monitors the operation of a host or network and alerts the system management when security interference is detected. Although the technology of intrusion detection system in common networks has matured, the current methods are not sufficient for IoT systems, the specific characteristics of IoT affect how it is developed [2]. The storage and processing capacity of network nodes that host system agents is very important, in common networks, system management sends system agents to nodes with higher processing capabilities, Internet of Things networks have nodes with resource limitations, so finding nodes that can support agents It will be more difficult to have the system. Another problem is related to network architecture, in common networks, end systems are connected to specific nodes (wireless access points, switches, and modems) that are responsible for sending packets to their destination. IoT networks are usually multi-hop, so common nodes may send packets and be end systems at the same time. For example, in the lightweight - light system equipped with the internet, motion detectors are hooked on the beam, and the refocused database is transferred by



.

Figure 1. The number of cyber attacks in the period from 2016 to 2021

sensors to the bulb's location to get at the entrance to the internet. This kind of architecture is a challenge to identify the computer. The last problem is the network's protocols. the immune system uses protocols that are not used [3].

2. Intrusion Detection Model based on Convolutional Neural Network

Signature-based Intrusion Detection Systems (IDS): These systems detect intrusions by comparing network traffic against a database of known attack signatures. If a match is found, an alert is generated. Signature-based IDS are effective against known threats, but they cannot detect new or unknown attacks.

Anomaly-based Intrusion Detection Systems (IDS): These systems detect intrusions by analyzing network traffic patterns and identifying deviations from normal behavior. Anomalies are flagged as potential attacks, and alerts are generated. Anomaly-based IDS are better at detecting new or unknown attacks, but they can generate false positives due to normal network variations[4].

Statistical-based Intrusion Detection Systems (IDS): These systems use statistical analysis to detect intrusions by identifying deviations from normal network behavior. They analyze network traffic patterns and identify anomalies based on statistical distributions. Statistical-based IDS are effective at detecting both known and unknown attacks, but they can generate false positives due to normal network variations [5].

Behavioral-based Intrusion Detection Systems (IDS): These systems detect intrusions by analyzing user and system behavior to identify deviations from normal patterns. They learn normal behavior through machine learning algorithms and flag deviations as potential attacks. Behavioral-based IDS are effective at detecting both known and unknown attacks, but they require a significant amount of training data to learn normal behavior.

Network Traffic Analysis (NTA): NTA is a network security approach that uses machine learning algorithms to analyze network traffic patterns and identify potential threats. It can detect both known and unknown attacks by identifying anomalies in network behavior. NTA is effective at detecting advanced persistent threats (APTs) and other sophisticated attacks.

Deep Learning-based Intrusion Detection Systems (IDS): These systems use deep learning algorithms to analyze network traffic patterns and identify potential threats. They can detect both known and unknown attacks by identifying complex patterns and relationships in network behavior. Deep learning-based IDS are effective at detecting advanced threats, but they require significant computational resources and training data.

Hybrid Intrusion Detection Systems (IDS): These systems combine multiple intrusion detection techniques to provide a more comprehensive and effective detection capability. They can detect both known and unknown attacks by using a combination of signature-based, anomaly-based, statistical-based, behavioral-based, and deep learning-based techniques. Hybrid IDS are effective at reducing false positives and improving overall detection accuracy [6].

3. Deep Learning

Many definitions of deep learning have been put forward by different researchers. Nonetheless, they all have commonalities and common keywords, such as «complex arhitectural data model», «unsupervised machine learning», «learning multiple layers», and «nonlinear data transformations» These key terminologies are all closely associated with neural networks and pattern recognition. In general, deep learning does not require pre-selected features, which overcomes the issue of feature selection because deep learning automatically extracts significant features from raw input to address the problem at hand. Deep learning models usually involve various processing layers consisting of multiple abstraction levels, enabling the system to learn various data features. The inclusion of multiple levels allows the network to remember distinct features [7]. Deep learning has been widely recognized as an approach that generates promising outcomes in various fields, including image recognition, speech recognition, face recognition, language translation, topic classification, sentiment analysis, signal processing, and natural language processing. Moreover, many different deep learning architectures have been developed, such as DBNs, RNNs, and CNNs.

3.1. Convolutional Neural Network

A CNN is a deep learning model used to process data such as images, and it is based on the arrangement of the animal visual cortex It is primarily designed to automatically and adaptively learn the spatial hierarchies of features in low- to high-level patterns . It has been proven to be effective in several tasks, including face identification, object identification, and traffic sign detection, most notably in robotics and self-driving cars [8]. Minimizing the number of parameters in an ANN is the most critical aspect of a CNN, which has motivated developers and researchers to focus on larger models that can be used to solve complicated tasks, which is impossible with traditional ANNs.The key purpose of a CNN is to learn the relevant features of the input data. In this process, the initial layers are a set of convolutional feature extractors that are subjected to learnable filters. The applied filters serve as a sliding window that moves across every piece of input data. In this case, the overlapping distance is referred to as the stride, with the outputs being known as feature maps [9]. Convolutional kernels make up each CNN layer, which is used to make different feature maps. Neighboring neuron areas are connected to a neuron in the next layer’s feature map. To create a feature map, the kernel must be shared across all spatial locations of the input. After the convolutional and pooling layers have been established, one or several fully connected layers are utilized to finish the classification.

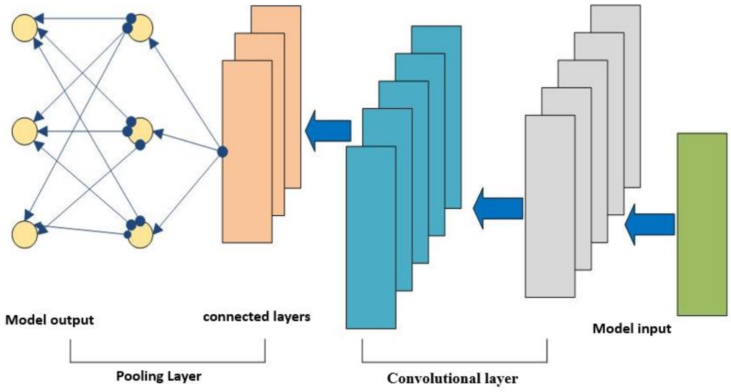


Figure 2. Convolutional neural network structure.

3.2. Convolutional layer

The convolution layer is the main building block of a network and is where most of the computations are done. This includes the input data and the convolutional filter. A data feature detector, also known as a kernel or filter, moves the image receiver fields and checks if the feature is present. This process is known as a complication. The following filter is part of the image [7] and is a matrix that moves over the input image and selects the grid between the input pixels and the filter to obtain an output array. The resulting output array is selected as the data attribute. Figure 2 shows the convolution operation between the input image and the kernel [10].

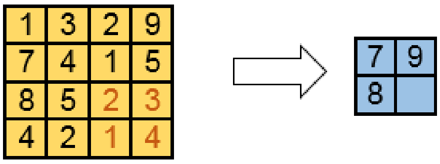


Figure 3. Twisting mathematical operations

3.3. Pooling layer

Sampling layers in a convolutional network are used to summarize data features during downsampling, as this allows us to access deeper layers of the network. When we reach the end of each stage and want to perform downsampling, the storage capacity decreases. Therefore, to store this information, it must be sampled to make a summary. The two most common types of sampling are incremental and averaging [11]. There is a lot of discussion among the research community about the best of each of the techniques of maximum increment and averaging [5]. The difference between the two types is that incremental sampling is used throughout the network to preserve the best features; But averaging at the endpoints is used to get the features before the last dense layer, and then everything is handed over to the mathematical function of the maximum smooth function.

3.4. Fully connected layer:

Smoothing is used to transform 2D arrays of maps into a continuous linear vector. The smoothed matrix is converted as input to the fully connected layer for image classification.

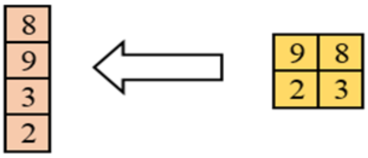


Figure 4. Smoothing grid arrays

These connected layers connect the neuron in one layer to the neuron in the other layer and the multiperceptron layer [6]. After several layers of convolution and merging the output, the vector is obtained through the connected layer.

4. Optimization Algorithm

The framework should be designed to ensure security and be compatible with organizational security needs. An intrusion detection system model can be created using any combination of classification method and the model should meet performance criteria such as accuracy, detection rate, false alarm rate. In the figure below, you can see the network implementation diagram in this article. First, we select the input data to the system [10]. In the next step, considering that the data should be statistically compared and the data that cause incorrect results should be removed. In the next step, we perform statistical tests on the data to make sure that the data is standard and normal. Now it's time to train the neural network model [12]. We have to give standardized data to the model so that it can be trained using them. The last step using the data which the model has not experienced before, we evaluate the proposed model to see if the model is properly trained.

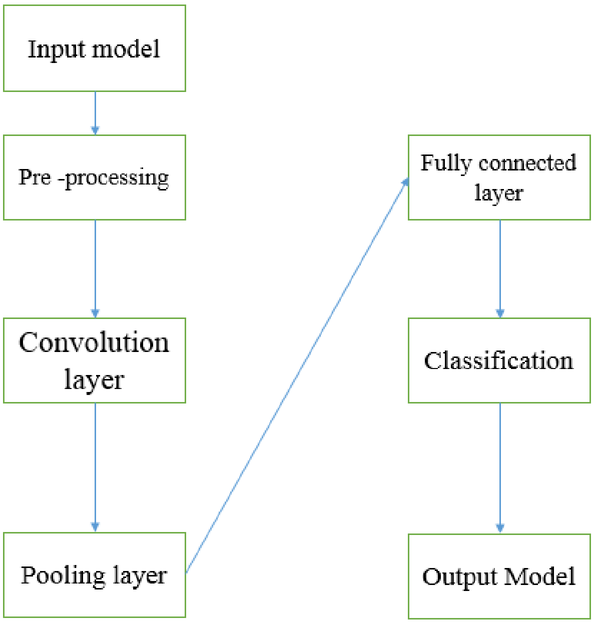


Figure 5. The steps of using the torsion network

5. Data processing process:

In 1998, the DARPA Intrusion Detection Evaluation Program was developed and managed by Lincoln Laboratory at the Massachusetts Institute of Technology. Their goal was to review and evaluate intrusion detection equipment. They simulated a standard dataset containing a large number of normal and abnormal network traffic. The standard dataset for intrusion detection called KDD CUP is the version used for modeling in this research [11]. The KDD CUP dataset is a well-known example of intrusion detection techniques. Much research is being developed to improve intrusion detection techniques, while research on the data used to train and test detection models is very important, as better data quality can improve intrusion detection. For its experiment, Lincoln Laboratory implemented an environment for receiving raw data that resembles the US Air Force LAN. The network worked exactly like the Air Force Network, but was tested in several attacks. The raw test data was approximately 4 GB, consisting of raw data obtained from network traffic. This data is the result of processing 5 million call data in this network [13]. A connection that starts and ends at a specific time and the data transfer flow from the source address to the destination address is performed according to a known protocol. In the NSL-KDD dataset, each entry has 43 fields. 41 characteristics, a closed behavior field that specifies the type of intrusion, and the last field indicates the degree of difficulty in detecting the intrusion. The tag column has 5 categories, a general category and 4 penetration categories including DoS, U2R, R2L and Prob. In a denial of service attack, a large overhead is created on the server by saturating the machine with many communication requests, preventing the server from responding to legitimate network traffic. In the following, some of these features and data values are explained in the table.

Table 1.NSL-KDD training and testing dataset

File	Description	Num. of Samples	Num. of Normal
Train+	Full training set	125,973	67,343
Train20	20% of the training set	251,92	13,499
Test+	Full testing set	22,544	9711
Test–	A subset of training set	11,850	2152

5.1. Data normalization

In the NSL-KDD dataset, there are three features that are qualitative and the rest are numerical. Since the input values must be numeric, we convert qualitative features to numeric. For example, the "protocol_type" attribute can have three different types, which are "tcp", "udp" and "icmp". We encode them in binary form. The binary vectors are (0, 0, 1), (0, 1, 0) and (1, 0, 0.). Normalization has several features in the data set between the maximum and minimum values in which there is a difference. In this research, the logarithmic scaling method is used to reduce the differences, and then the following formula is used to map them to the range [0,1].

$$x_i = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

6. Using statistical tests for features

Standard processes such as data cleaning and preprocessing, classification, regression, and removal of outliers are used for classification. In the NSL-KDD dataset, the dataset includes different classes of attacks, namely DoS, R2L, U2R, and Prob. We explain these statistical methods in order:

6.1. Data processing

Processing is usually automatic and is performed on a computer. When data contains information, data processing systems are often called information systems to emphasize their practicality. However, these terms are generally synonymous and represent similar transformations, data processing systems commonly transform raw data into information, and similarly information systems take raw data as input to produce information as output. Data can be viewed as a raw material that is later transformed into information. For example, a factory will need raw materials or raw materials to produce its final product in order to reach the final product that will be used. Meanwhile, according to the type of raw material and the final product, different processes and different stages are performed on the raw material. These steps are similar to the steps mentioned for data processing, an information system takes the raw material (initial data) and after processing and preparing it - which is called processing - turns the raw material into the final product (information) and as output to be used. As it is known, the processing steps for a car manufacturing plant are different from the processing steps of an industrial equipment manufacturing plant; In information systems, the processing steps will differ according to the type of primary data and desired information. When the field from which the data is extracted is science or engineering, data processing and information systems are very broad terms; The term more specialized data analysis will usually be associated with a greater focus on highly specialized and precise algorithmic derivations and complex computations that are less commonly seen within the scope of work environments.Outlier data: Outlier data or outlier data in the subject of statistics is a data that has a significant distance from other data of the same group. An outlier is defined as follows: an outlier is a data that is significantly different from the rest of the sample in which it occurred. A particular data as well as other outlier data can exist for many reasons; But their presence usually indicates that; Either some measurements have errors, or the data has a heavy-tailed probability distribution (point indicator).

6.2. Linear regression

A statistical model for predicting one or more variables from one or more other variables. The variables that are predicted are called dependent variables and the variables that are predicted with the help of them are called independent variables. If there is only one independent variable, the linear regression model is called simple, otherwise it is called multiple. Also, if several dependent variables are predicted instead of predicting one dependent variable, the linear regression model is called multivariate. More precisely, he used the term "regression to the mean" to describe this relationship. If the dependent variable takes numerical values, the modeling problem is called "regression", and otherwise (when the dependent variable is ordinal) it is called "statistical classification".

7. Feature selection

There are many feature selection techniques, in our proposed model, we use the torsional nerve network to select the relevant features . the network structure consists of multidimensional layers with multiple normal layers. the idea is to use the torsional layer and the maximum integration layer for parameter sharing, spatial arrangement, and the characteristics of local perception. parameter sharing allows a reduction of a set of parameters and variables that result in feature extraction using less processing resources. the layout of a matrix indicates a better detection of the correlation between the data.

8. Training and Test model

This model was tested using KDDTrain +. TXT, which 80 percent is used for training and 20 percent for validation, and finally KDDTest + . TXT is used for model testing. in the following figure you will see a portion of the model that has been implemented.

9. Experimental Evaluation

We use accuracy evaluation criteria to measure the performance of the model. Accuracy is how close the measured value is to the true value.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \tag{2}$$

In addition, we also calculate false positive and detection rates. Positive rate numbers indicate records that are correct again It works and is recognized as an anomaly.

$$DR = TPR = \frac{TP}{TP + FN} \tag{3}$$

The false positive rate is a measure of the accuracy of a test: whether it is a diagnostic test or a machine learning model. In technical terms, the false positive rate is defined as the probability of falsely rejecting the null hypothesis.

$$FPR = \frac{FP}{FP + TN} \tag{4}$$

10. Results and discussion

The experiments are conducted using TensorFlow on Windows, where the code is written in Python. The model is trained for 100 iterations, and hyperparameter tuning is performed. The training is done using the KDD-Tain dataset, and the results show an accuracy of 98.2% and a false positive rate of 0.1%.

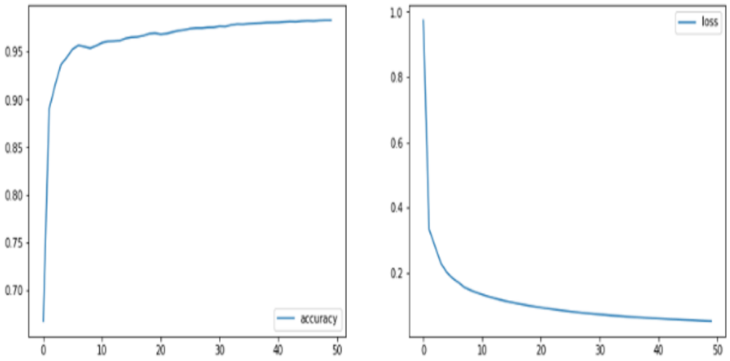


Figure 6. Accuracy values

For model validation, 20% of the KDD-Tain dataset is set aside for validation purposes. In the end, the KDD-Test dataset is fed into the model for final evaluation. To obtain better results, the dataset is split into two parts for more accurate analysis.

Table 2. Results of intrusion detection model

	Accuracy evaluation criteria	**True positive rate**	**False positive rate**
KDD-Test	92.3	88.5	3.2
KDD-Test 20	88.5	76.3	5.4

The evaluation metric for KDD-Test is accuracy, which is 92.3% for the full KDD-Test dataset and 81.5% for the first 20% of the KDD-Test dataset. The true positive rate (TP Rate) for KDD-Test is 92.3% and the false positive rate (FPR) is 7.7% for the full KDD-Test dataset, and for the first 20% of KDD-Test dataset, the TPR is 81.5% and the FPR is 12.5%. The specificity (SPR) for KDD-Test is 92.3% and for the first 20% of KDD-Test dataset, the SPR is 87.5%. The precision (PR) for KDD-Test is 92.3% and for the first 20% of KDD-Test dataset, the PR is 81.5%.

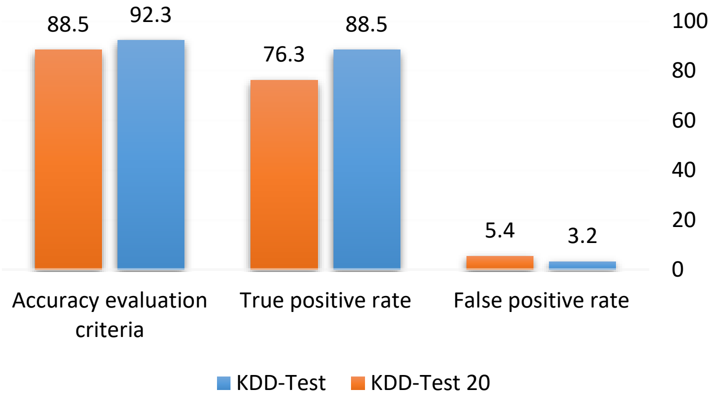


Figure 7. Model results

In the following table, the results of using the deep learning approach, as well as other methods such as random forests, decision trees, and other classification algorithms, are compared to identify the best models that can provide accurate results and effectively detect anomalies. The results show that the model's accuracy for KDD-Test 20 is around 78.3%, while the accuracy for KDDTest+ is approximately 92.3%.

Table 3. Results and comparison of intrusion detection models and performance of convolutional model and other machine learning models.

	KDD Test+	KDD Test-20
Naïve bayes	84.4	71.1
NB Tree	79.6	61.3
Random Forest	80.5	68.9
Svm	75.3	50.96
RNN	81.2	64.12
CNN	92.3	78.3

This indicates that the CNN model is more effective in detecting anomalies and provides more accurate results compared to other methods

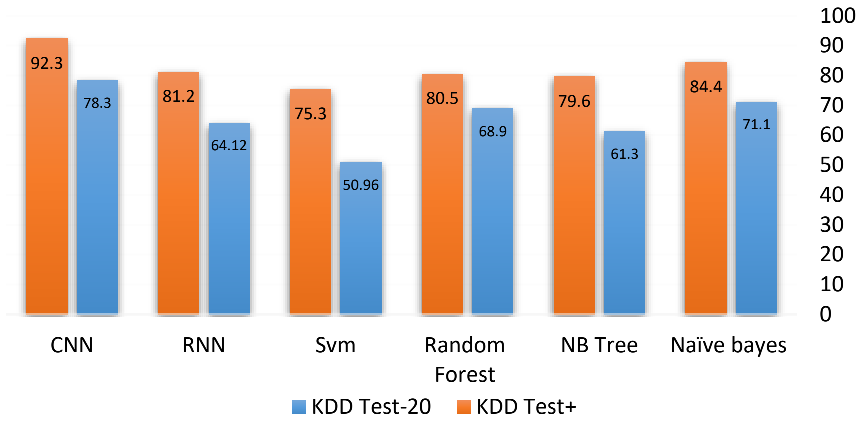


Figure 8. Results of intrusion detection models

11. Conclusion

The proposed model is implemented using Python and the TensorFlow framework. The model consists of multiple layers, including input, hidden, and output layers. The input layer receives the features extracted from the network traffic data. The hidden layers perform nonlinear transformations of the input data, and the output layer generates the predicted probability of a network attack. The model is trained using the Adam optimizer and the binary cross-entropy loss function. The learning rate is set to 0.001, and the batch size is set to 128. The model is trained for 100 epochs, and the best model is se lected based on the validation accuracy. The model is evaluated on the NSL-KDD dataset, which consists of 49,402 instances, including 20,307 normal instances and 29,095 attack instances. The model achieves an accuracy of 92.3% on the test set and a precision of 88.5%. Compared to other methods, the proposed model shows better performance in terms of accuracy and precision. The proposed model can be integrated into network intrusion detection systems to provide real-time predictions of network attacks. The model can also be fine-tuned for specific types of network attacks or network environments. The model's performance can be further improved by incorporating more features or using different optimization algorithms. In summary, the proposed model is a deep learning-based approach for network intrusion detection using the NSL-KDD dataset. The model achieves high accuracy and precision, making it a promising solution for network intrusion detection.

References

[1] Hasan, M., et al. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things, 7*.

[2] Asghari, R., & Semyari, R. (2022). A Mutual Lightweight Authentication Protocol for Internet of Things Environment Using smart card. *Computational Sciences and Engineering, 2(1)*, 41-52.

[3] Jiang, J., et al. (2022). A dynamic ensemble algorithm for anomaly detection in IoT imbalanced data streams. *Computer Communications, 194*, 250-257.

[4] Ever, Y. K., B. Sekeroglu, B., & Dimililer, K. (2019). Classification analysis of intrusion detection on NSL-KDD using machine learning algorithms. *International Conference on Mobile Web and Intelligent Information Systems, Springer*.

[5] Asghari, R. (2021). A modified continuous lightweight authentication to increase the information security on internet of Things. *Computational Sciences and Engineering, 1(2),* 109-121.

[6] Muniyandi, A.P., Rajeswari, R., & Rajaram, R. (2012). Network anomaly detection by cascading k-Means clustering and C4. 5 decision tree algorithm. *Procedia Engineering, 30*, 174-182.

[7] Tobiyama, S., et al. (2016). Malware detection with deep neural network using process behavior. *IEEE 40th annual computer software and applications conference (COMPSAC).*

[8] Li, F., et al. (2014). Event-centric situation trust data aggregation mechanism in distributed wireless network. *International Journal of Distributed Sensor Networks, 10(8),* 585302.

[9] Masoodi, F. (2021). Machine Learning for Classification analysis of Intrusion Detection on NSL-KDD Dataset. *Turkish Journal of Computer and Mathematics Education (TURCOMAT). 12(10),* 2286-2293.

[10] Ingre, B., Yadav, A., & Soni, A.K. (2017). Decision tree based intrusion detection system for NSL-KDD dataset. *International conference on information and communication technology for intelligent systems. Springer.*

[11] Su, T., et al., (2020). *BAT:* Deep learning methods on network intrusion detection using NSL-KDD dataset. *IEEE Access, 8*, 29575-29585.

[12] Pourghaffari, A., Asghari, R., & Rashidi, A.J. (2022). Toward Cyber Command and Control System Architecture Using Data-Driven Analysis Solutions. *Computational Sciences and Engineering, 2(1),* 53-68.

[13] Pascanu, R., et al. (2015). Malware classification with recurrent networks. *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).*