Hindawi
Security and Communication Networks
Volume 2021, Article ID 6129210, 12 pages
https://doi.org/10.1155/2021/6129210

WILEY | Hindawi

Research Article

Deep Learning-Based Framework for the Detection of Cyberattack Using Feature Engineering

Muhammad Shoaib Akhtar and Tao Feng

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Correspondence should be addressed to Tao Feng; fengt@lut.cn

Received 4 September 2021; Revised 6 November 2021; Accepted 18 November 2021; Published 24 December 2021

Academic Editor: Marimuthu Karuppiah

Digital systems are changing to security systems in contemporary days. It is time for the digital system to have sufficient security to defend against threats and attacks. The intrusion detection system can identify an anomaly from an external or internal source in the network system. Many kinds of threats are present, that is, active and passive. These dangers could lead to anomalies in the system by which data can be attacked and taken by attackers from the beginning to the destination. Machine learning nowadays is a developing topic; its applications are wide. We can forecast the future through machine learning and classify the right class. In this paper, we employed the new binary and multiclass classification model of Convolutional Neural Networks (CNNs) to identify the anomaly of the network system. In this respect, we used the NSLKDD dataset. Our model uses a Convolutional Neural Network (CNN) to conduct binary and multiclass classification. In both datasets, we build a DL-based DoS detection model. We focus on the DoS category in the most extensively used IDS dataset, KDD. As the name implies, CNN is the most extensively used the DL model for image recognition. Adding a pooling layer to the convolution layer minimizes the size of the feature data extracted from the image while maintaining I/O and spatial information. The CNN model has shown the promising results of multiclass and binary classification in terms of validation loss of 0.0012 at 11th epochs and validation accuracy of 98% and 99%, respectively.

1. Introduction

As computer network traffic and sensitive information on network systems grow, more firms are becoming vulnerable to a wider spectrum of attacks. The subject of how network systems might be protected from infiltration, disruption, and other abnormal actions of undesirable attackers is crucial [1]. Traditional intrusion prevention measures, like firewalls, access control, and SNP, and encryption technologies cannot always defend network systems because hostile traffic is channeled into the system [2].

The IDS [3] is an integral part of the security architecture that may be used to detect and identify threats and to monitor intruders. Internet Organized Crime Threat Assessment (IOCTA), Europol's fourth annual presentation of the European Cyber Crime Center's cybercrime threat picture, was released in 2016 and mid-2017 (EC3). As indicated by many big attacks between the end of 2016 and the middle of 2017, cybercrime has been shown to be growing and emerging and taking new paths [4].

A large number of gadgets are connected to the Internet and, thanks to the continual development of the Internet, communicate in real time. The Social Internet of Things (SIoT) (2) can offer people omnipresent Internet connectivity that combines social behavior with a physical Internet of Things (IoT) [5]. Through the broad application of SIoT, millions of sensors or devices continue to generate and share critical information [6]. Collaborative edge computer (CEC) is increasingly used by services providers to reduce the problem of resource congestion [7], which migrates data computation and storage to a network edge in close proximity to the users [8]. Figure 1 shows the basic terminology of the intrusion detection system.

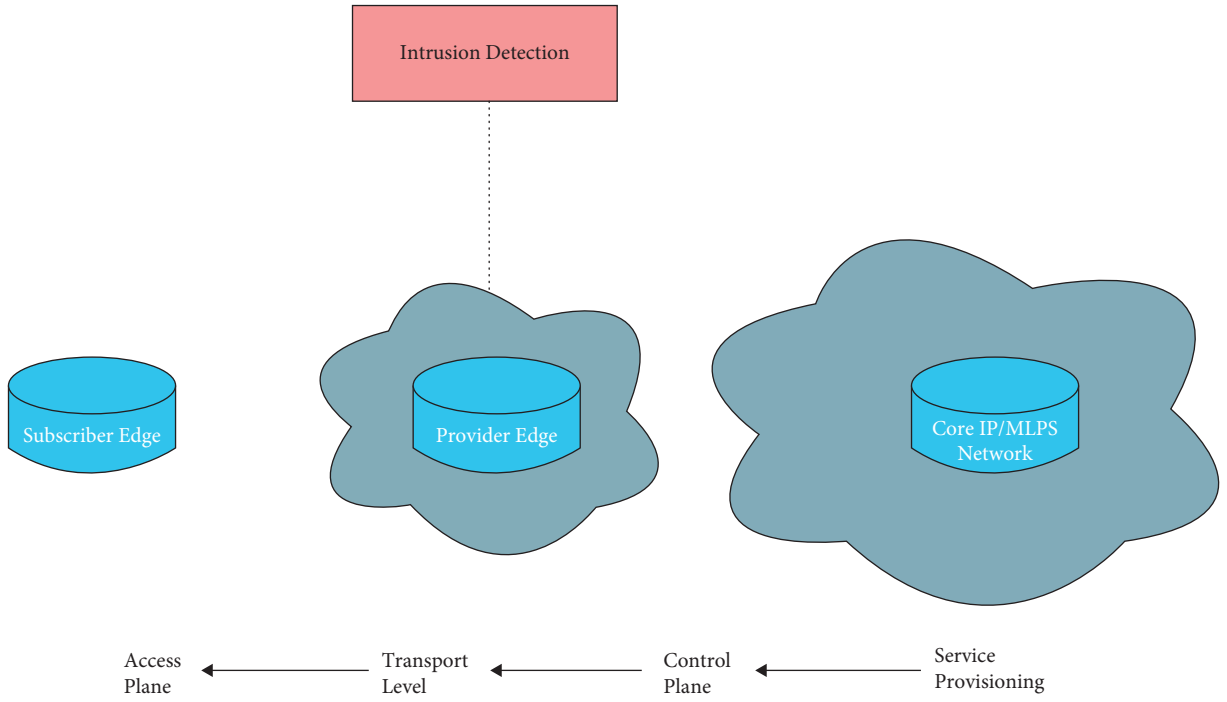

Figure 1: Basic terminology of the intrusion detection system.

For decades, anomaly detection has been a hot topic, with numerous applications in industries such as fault tolerance, financial and economic crisis detection, health diagnosis, extreme phenomena in Earth science and meteorology, atypical celestial object detection in astronomy or astrophysics, and system intrusion in cybersecurity [9–12]. The difficulty of detecting patterns that depart from a "normality" behavioral model is known as anomaly detection. The majority of approaches in the literature can be classified either by the model of normality used or by how they approach abnormality characterization and identification. The study in [1] proposes a comprehensive, albeit somewhat outdated, review of anomaly detection, which is followed by a more recent comparison analysis [13–15].

The basic concept behind the method of isolating the forest is that, in general, isolating an "outlier" from the given data is much easier than isolating an "inlier" from the remainder. Convolutional Neural Networks select a feature randomly from a group of features, then select a range between maximum and minimum values of the selected feature, and then randomly select the split values of the minimum and maximum values of the selected features. Figure 2 shows the result of applying the Convolutional Neural Network on a real-time web-based system, which can potentially detect anomalous points in the given web traffic. In Figure 2, an example of web traffic with some anomalous points has been represented.

Figure 3 shows the idea behind isolating the forest in a random forest to split the features of the selected feature set. The anomaly score using a Convolutional Neural Network can be calculated as follows:

$$c(m) = \begin{cases} 2H\,(m-1) - \dfrac{2\,(m-1)}{n} \ldots \text{for } m > 2, \\ 1 \ldots \text{for } m < 2, \\ 0 \ldots \text{otherwise.} \end{cases} \quad (1)$$

In equation (1), $c\,(m)$ is the anomaly score and H is the harmonic feature whose range for splitting the maximum and minimum values has been settled between less than and greater than 2. Figure 3 shows the basic idea behind anomaly detection using Convolutional Neural Network trees.

Because of the likelihood of hostile traffic being injected into the system, traditional intrusion prevention methods like firewalls, access control, and secure network protocols (SNP), and encryption cannot always keep network systems safe. An integral part of the security infrastructure, which helps to detect and identify threats, as well as monitor intruders, is the intrusion detection system (IDS) [13, 14, 17–19].

IDS is a famous and successful network security system, which offers security and safety for the transfers on network systems [20–22]. Most work [23–25] has tackled issues such as overfitting, replication, high-dynamics, and a small number of instances of workouts. For this purpose, we have used machine learning techniques to predict the types of attacks and anomalies in the security system.

Since typical machine learning algorithms are poorly generalized, deep learning algorithms take more time and are likely to disappear gradually or explosively. Although technology based on deep neural networks can tackle the

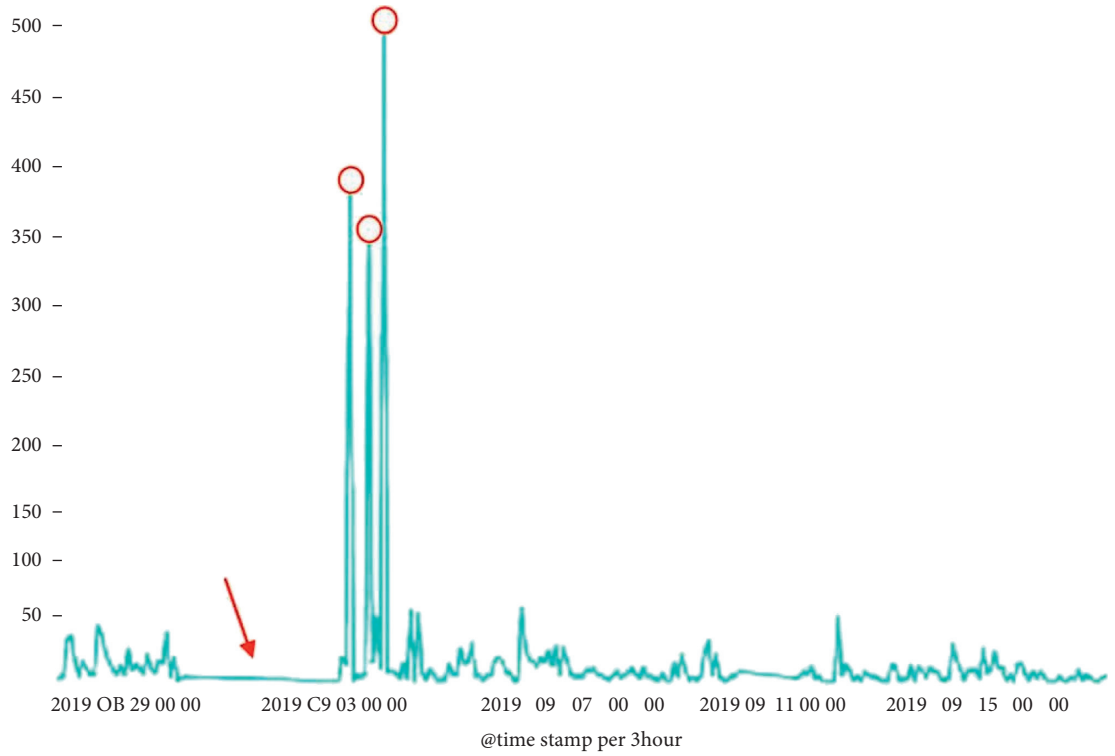

Figure 2: Web traffic with potentially anomalous points [16].

problem of time-consuming and unknown attacks, the pretraining model still undergoes deep-school gradient disappearance or explosion. Finalizing a deep residual neural network can handle these difficulties at the same time.

The core contributions of this research are as described as follows:

(i) For an intrusion detection system, we use a unique architecture called Convolutional Neural Networks (a form of decision tree) (IDS).

(ii) No other IDS researcher has implemented the multiclass and binary classification model of Convolutional Neural Networks in line with what we have observed in recent studies.

(iii) The CNN reduces the sparsity-related objective cost function of IDS classification.

(iv) The IF displays numerous features exceptionally suited to IDS, including high accuracy, detection rate, training time for model creation, and average training time per sample.

(v) We have built a new CNN-based intrusion detection system. The CNN-based technique can extract low-dimensional features for functional training from the original network streams.

(vi) There is no great accuracy in intrusion detection for detecting repeated attacks.

(vii) We build a CNN-based method that may be used to accurately capture diverse forms of attacks.

(viii) We create several CNN-based intrusion detection systems. The proposed system can detect a number of new sorts of assaults through existing types of attacks.

2. Literature Review

This section discusses the present intrusion detection system strategies. The material now available is generally classed into supervised and unattended learning strategies.

Nowadays, the ever-increasing sophistication and severity of security attacks on computer networks have encouraged security experts to use diverse machine learning technologies to secure the organizations' data and reputation. Deep learning is one of the interesting techniques which recently have been extensively adopted by the IDS or intrusion detection systems to boost their performance in securing the computer networks and hosts. The review article in [1] focuses on deep learning-based intrusion detection techniques and puts out an in-depth survey and classification of these schemes. It first introduces the basic background principles concerning IDS architecture and several deep learning approaches. It then classifies these schemes according to the type of deep learning algorithms applied in each of them. It describes how deep learning networks are applied in the intrusion detection process to recognize intrusions accurately. Finally, a thorough analysis of the researched IDS frameworks is offered, and concluding observations and future directions are noted.

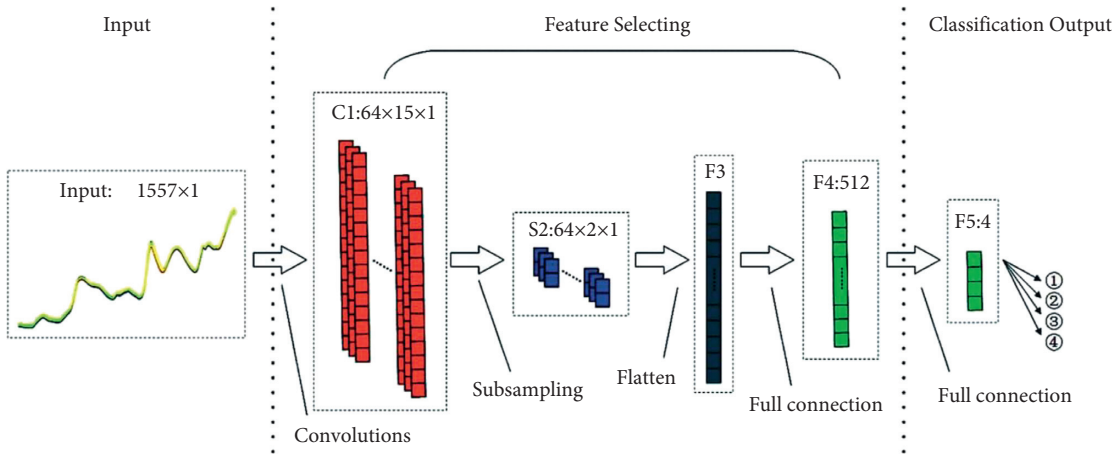

Figure 3: Basic idea behind anomaly detection using Convolutional Neural Network trees.

When balancing the sample distribution, Hu et al. [3] employ the ADASYN approach, which can successfully avoid the model from becoming sensitive to large samples while being insensitive to small samples. For the second time, the upgraded CNN is built on the split convolution module (SPC-CNN), which can increase the diversity of features while also reducing the impact of interchannel information redundancy on the model training process. Then, for intrusion detection tasks, an AS-CNN model that is a combination of ADASYN and SPC-CNN is used. Finally, the standard NSLKDD dataset is used for testing the AS-CNN algorithm. Compared to classic CNN and RNN models, the simulation shows that the accuracy is 4.60 percent and 2.79 percent higher, respectively, and that the detection rate (DR) has grown by 11.34 percent and 10.27 percent, respectively. Additionally, the FAR reduced by 15.58 percent and 14.57 percent, respectively, when compared to the two models under consideration.

Yang et al. [4] ran a sample test to see how the network would react if it were attacked by an intruder. In our paper's simulations, the authors demonstrate that the method proposed has higher detection accuracy and true positive rate, as well as a lower false positive rate, when compared to other methods. The test results on the test set KDDTest + in this paper show that when compared with the traditional models, the detection accuracy of LeNet-5 and DBN is 8.82 percent and 0.51 percent higher, respectively, and the recall rate of LeNet-5 and RNN is 4.24 percent and 1.16 percent higher, respectively, while the false positive rate is lower than the other three types of models (LeNet-5, RNN, and RNN).

It is proposed in research [5] that a novel ensemble intrusion detection method is used to defend network assaults against the train ECN, namely, IP Scan, Port Scan, Denial of Service (DoS), and Man in the Middle attacks (MITM). The raw data generated by our ECN testbed are processed to extract thirty-four features of distinct protocol contents, which are then combined to make a specific dataset. The dataset will be optimized through the use of a data imaging approach and a temporal sequence construction method. On the basis of various typical Convolutional Neural Networks and recurrent neural networks, six base classifiers are constructed: the LENET-5 (also known as AlexNet), the VGGNet (also known as SimpleRNN), the LSTM (also known as LSTM-R), and the GRU (also known as GRU-R). To incorporate all of the base classifiers, it is recommended to use a dynamic weight matrix voting approach. The proposed method is evaluated in light of the data authors have collected. In the experiments, the findings demonstrate that the proposed technique has an exceptional capacity for aggregating the advantages of all base classifiers and that it achieves superior detection performance with an accuracy of 0.975.

Kim et al. [6] proposed the Artificial Intelligence-Based Intrusion Detection System (AI-IDS) that was installed and put into use. With the help of an optimal Convolutional Neural Network and long short-term memory network (CNN-LSTM) model and normalized UTF-8 character encoding for Spatial Feature Learning (SFL), authors are able to adequately extract the characteristics of real-time HTTP traffic without the use of encryption, calculating entropy, or compressing the data in any way. Using repeated experiments on two publicly available datasets (CSIC-2010 and CICIDS2017) as well as fixed real-time data, authors established the system's superiority. AI-IDS identifies sophisticated assaults, such as unknown patterns and encoded or obfuscated attacks, from innocuous traffic by training payloads that analyze true or false positives with a labeling tool and then compare the results. It is a versatile and scalable system that is implemented using Docker images, with user-defined functions being separated into independent images by independent images. It also aids in the development and improvement of Snort rules for signature-based intrusion detection systems based on newly discovered patterns. It is possible to accurately assess unknown web attacks due to the fact that the model determines harmful likelihood through continual training.

An approach for network intrusion detection that combines hybrid sampling with deep hierarchical networks is proposed here. First, Jiang et al. [7] employ one-side selection (OSS) to lower the number of noise samples in the majority category, and then the authors employ Synthetic Minority Oversampling Technique (SMOTE) to increase the

number of minority samples. A balanced dataset can be created in this manner, allowing the model to completely learn the characteristics of minority samples while also significantly reducing the model training time. To extract spatial features, the authors utilize Convolution Neural Networks (CNNs), and to extract temporal features, the authors employ bidirectional long short-term memory (BiLSTMs), which are combined to produce a deep hierarchical network model. It has been demonstrated that the proposed network intrusion detection method is accurate on the NSLKDD and UNSW-NB15 datasets, with classification accuracy reaching 83.58 percent on the NSLKDD and 77.16% on the UNSW-NB15, respectively.

In this paper, Park et al. [8] describe an effective method for distinguishing between abandoned things, stolen objects, and ghost regions in the surveillance camera footage. For providing the object mask information, this method uses two main strategies: the first is a dual background model to extract candidate stationary objects, and the second is object segmentation based on mask regions with CNN features (Mask R–CNN) to extract candidate stationary objects from the background model. When given a candidate stationary item from the backdrop model, it is tested to see if an identical segmented object exists in the current video frame or the prior background frame in order to take into consideration both the present and previous conditions. And the ultimate state of the candidate stationary object is determined by taking into account a variety of different scenarios using the comparative analysis technique described in this paper, which is then applied. The suggested approach has been qualitatively tested with their own dataset, with particular attention paid to the discriminating problem, and the results have been good. Consequently, it is projected to be widely used in open environments such as exposition halls and public parks, where traditional intrusion detection-based security services are difficult to install, such as for automatic detection of stolen objects and abandoned items.

To improve the overall security of the Internet, the study in [26] proposes an intrusion detection system (IDS) based on the Convolutional Neural Network (CNN). The suggested intrusion detection system (IDS) is designed to identify network intrusions by categorizing every packet traffic in the network into benign and harmful classifications. The dataset CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection System) was used to train and validate the proposed model, which is available online. The model has been examined in terms of overall accuracy, attack detection rate, false alarm rate, and training overhead. The model was found to be accurate in all of these areas. A comparison of the suggested model's performance to the performance of nine other well-known classifiers is offered in this paper.

It is proposed in [27] to use a quantitative model of the interaction mode between ports as the basis for an intrusion detection system (IDS). Taking into account the arrival time distribution of traffic, the model provides a quantitative expression of Port Interaction Mode in Data Link Layer (PIMDL), with the goal of improving the accuracy and efficiency of intrusion detection by taking the arrival time distribution of traffic into account. The approach of phase space reconstruction and visualization is used to demonstrate the practicality of the model that has been proposed. An artificial neural network based on CNN and LSTM is being developed to mine the differences between normal and abnormal models, taking into consideration the characteristics of long and short sessions. As a result, a better intrusion detection algorithm based on a multimodel scoring mechanism is being developed to classify sessions in model space on the basis of this information. Furthermore, the experiments demonstrate that the quantitative model and the improved algorithm proposed can not only effectively avoid camouflaging identity information but also improve computational efficiency while simultaneously increasing the accuracy of small sample anomaly detection (as demonstrated by the experiments).

In order to tackle the aforesaid difficulties, we employ a selection technique to approximate discriminatory features of the IDS classification. This research presents a multiclass and binary classification model of CNN for a more efficient manner of finding abnormality.

3. Methodology

Unauthorized users, even insiders, are protected from a computer network by software that detects network intrusions. The purpose of the intrusion detector learning challenge is to develop a predictive model (i.e., a classifier) that can distinguish between "bad" and "good" connections (intrusions or attacks) (normal connections). In 1998, the DARPA Intrusion Detection Evaluation Program was created and led by MIT Lincoln Labs. The objective was to conduct a survey and evaluate intrusion detection research. A common collection of data for auditing was provided, which includes a variety of intrusions simulated in the setting of a military network. In the 1999 KDD intrusion detection challenge, a variation of this dataset was utilized. Using the CNN-based model, we can conduct binary classification and multiclass classification. The two datasets are used to construct a DL-based detection model for DoS assaults. In addition to KDD, the most extensively used IDS dataset, we pay particular attention to the DoS subcategory in both of these datasets. As far as image identification goes, CNN is the most often used DL model, consisting of a convolutional layer that extracts the image features and a fully connected layer that determines which class the input image falls into. Image features are extracted from the convolution layer while retaining I/O and spatial information and are reduced in size by using a pooling layer in conjunction with the convolution layer.

The raw training data was almost four terabytes of compressed binary TCP dump data collected over seven weeks of network traffic. This resulted in the creation of around five million connection records. Around two million connection records were created in two weeks of test data.

Validation of the process is done using performance criteria such as accuracy, AUC, sensitivity, and specificity.

The working flow of the proposed method using machine learning techniques is shown in Figure 4. The details of

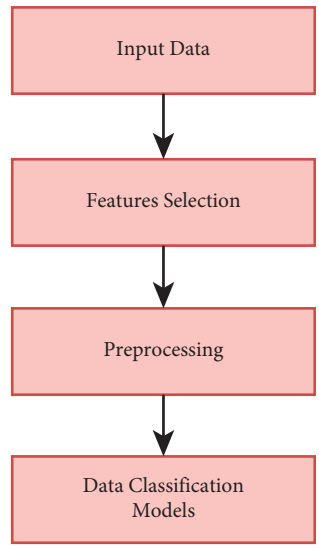

Figure 4: Block diagram of the proposed method.

the block diagram are as follows: The data have been split into testing and training to validate the results. The different machine learning models have been used; the purpose of each model or classifier is to generate a result in a hybrid way by using an optimization technique.

The NSLKDD network security dataset is used for testing and evaluation of the offered method. The NSLKDD dataset contains different real-world data for network systems. As we know, the data are in the raw form, so we have converted the raw data into CSV data file for preprocessing and feature extraction.

The following three tables provide a complete listing of the collection of features specified for the link logs. You will use a machine-readable data scheme for the contest dataset. Table 1 shows the basic features of individual TCP connections. While Table 2 shows the content features within a connection suggested by domain knowledge, Table 3 shows the traffic features computed using a two-second time window.

Figure 5 shows the categorical variables of traffic proportions. 46.54% are malicious, shown as "1," while normal instances are about 53.46%, represented as "0." In Figure 6, correlation features means per class has been shown. The maximum correlation has been shown with 1, and the minimum correlation has been shown with 0.

3.1. Feature Selection. Feature selection techniques are different from feature extraction as in feature selection, we have taken a subset of input features, and in the extraction of features, we can extract new features from existing features.

3.2. Feature Selection (Minimum Redundancy Maximum Relevance). In this case of feature selection, we select the features from data, which have the highest relevancy in predicting the output variable. And having minimum redundancy in the dataset, we can calculate the relevance of a feature set as follows:

$$D(S,c) = \frac{1}{|S|} \sum_{\text{fes}}^{n} I\ (fi, c). \tag{2}$$

In the following equation, *fi* and *fj* are the average of mutual redundant information between the subset of *fi* and *fj* feature set. Redundancy can be calculated as

$$R(S) = \frac{1}{|S|2} \sum_{fi,je\,S}^{n} I\ (fi, fj). \tag{3}$$

The following equation is used to find out the maximum relevance and redundancy in the feature selection:

$$\text{RMRM} = \max s \left\{ \frac{1}{|S|} \sum_{\text{fes}}^{n} I\ (fi; c) - \frac{1}{|S|2} \sum_{fi,je,s}^{n} I\ (fi, fj) \right\}. \tag{4}$$

There are many linear techniques for reducing dimensionality, but the principal component analysis is the most commonly used. It makes linear mappings of the data to lower-dimensional space in such a way as to optimize variance, which can be seen in Figure 7. Figure 8 shows the variables' ratio in terms of variance. There are a total of 37 variables; the highest variance ratio of variable "1" is 0.180.

This variance ratio can be used to see how each of the data's primary components contributes to the variance in data. Scree plots are a visual method for determining how many of the main components want to retain in the study, which can be seen in Figure 9.

For dealing with categorical information, label encoding is a popular encoding approach. Using this method, an integer is assigned to each label depending on its alphabetical order. Figure 10 shows the Visualization of Traffic in Time using Label Encoder.

Table 1: Basic features of individual TCP connections.

Feature name	Description	Type
Duration	Duration (sec number) of a protocol link	Continuous
Protocol_type	Type, for example, tcp and udp, on destination	Discrete
Service	Network service, for example, http and telnet	Discrete
src_bytes	Data bytes number from source to destination	Continuous
dst_bytes	Destination to source numbers of data bytes	Continuous
Flag	Regular or link error status connection	Discrete
Land	1 if the link is to/from the same host/port; 0 if not	Discrete
Wrong_fragment	Number of fragments "false"	Continuous
Urgent	Number of urgent packets	Continuous

Table 2: Content features within a connection suggested by domain knowledge.

Feature name	Description	Type
hot	Number of "hot" indicators	Continuous
num_failed_logins	Amount of unsuccessful login attempts	Continuous
logged_in	1 if signed in successfully; 0 otherwise	Discrete
num_compromised	Amount of "committed" conditions	Continuous
root_shell	1 if root shell has been obtained; 0 otherwise	Discrete
su_attempted	1 if the "your root" command was attempted; 0 otherwise	Discrete
num_root	Number of kinds of "root" access	Continuous
num_file_creations	Number of file generation operations	Continuous
num_shells	Range of prompts for shell	Continuous
num_access_files	Amount of access control files operations	Continuous
num_outbound_cmds	Number of outbound commands in the ftp session	Continuous
is_hot_login	1 if the username is a "hot" login; 0 otherwise	Discrete
is_guest_login	1 if the username is a "guest" login; 0 otherwise	Discrete

Table 3: Traffic features computed using a two-second time window.

Feature name	Description	Type
count	Amount of connections to the same host as the existing link in the last two seconds Note: these same host connections apply to the following functions	Continuous
serror_rate	Percent of links with "SYN" errors	Continuous
rerror_rate	Percent of connections with "REJ" errors	Continuous
same_srv_rate	Percent of connections with the same service	Continuous
diff_srv_rate	Percent of links to various networks	Continuous
srv_count	Amount of connections to the same service as the existing link in the last two seconds Note: these same service links are referred to as the following functions	Continuous
srv_serror_rate	Percent of links with "SYN" errors	Continuous
srv_rerror_rate	Percent of connections with "REJ" errors	Continuous
srv_diff_host_rate	Percent of connections between different hosts	Continuous

3.3. Convolutional Neural Networks. The simple concept behind this approach to CNN is, in general, that isolating an "outlier" from the other data is much easier than isolating an "inferior" of the remainder of the data. With the help of a Convolutional Neural Network (CNN), we can conduct binary classification and multiclass classification with the model we have developed. In the two datasets, we create a DL-based detection model for Denial of Service (DoS) assaults. We concentrate on the DoS category in not just the KDD dataset, which is the most extensively used IDS dataset, but also in other datasets. Cannon's Convolutional Neural Network (CNN) is the most extensively used deep learning model for image identification. It is composed of a convolution layer that extracts the properties of an image and a fully connected layer that identifies which class the input image belongs to. Convolution layers extract the unique features of an image while maintaining the I/O and spatial information of the image. Adding a pooling layer to the convolution layer helps to minimize the size of the feature data by combining it with the previous convolution layer.

4. Results and Discussion

This section is about the model evaluation and results of this research work. In this section, we will discuss the accuracy of our model. We will try both multiclass and binary classification. In the case of binary, we will cluster all malicious

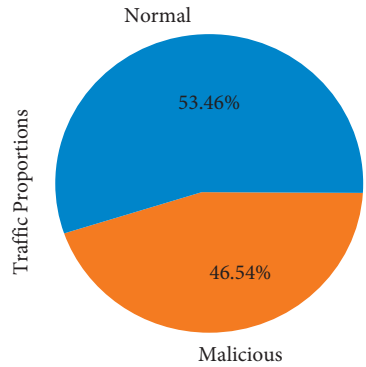

Figure 5: Dataset categorical variables.

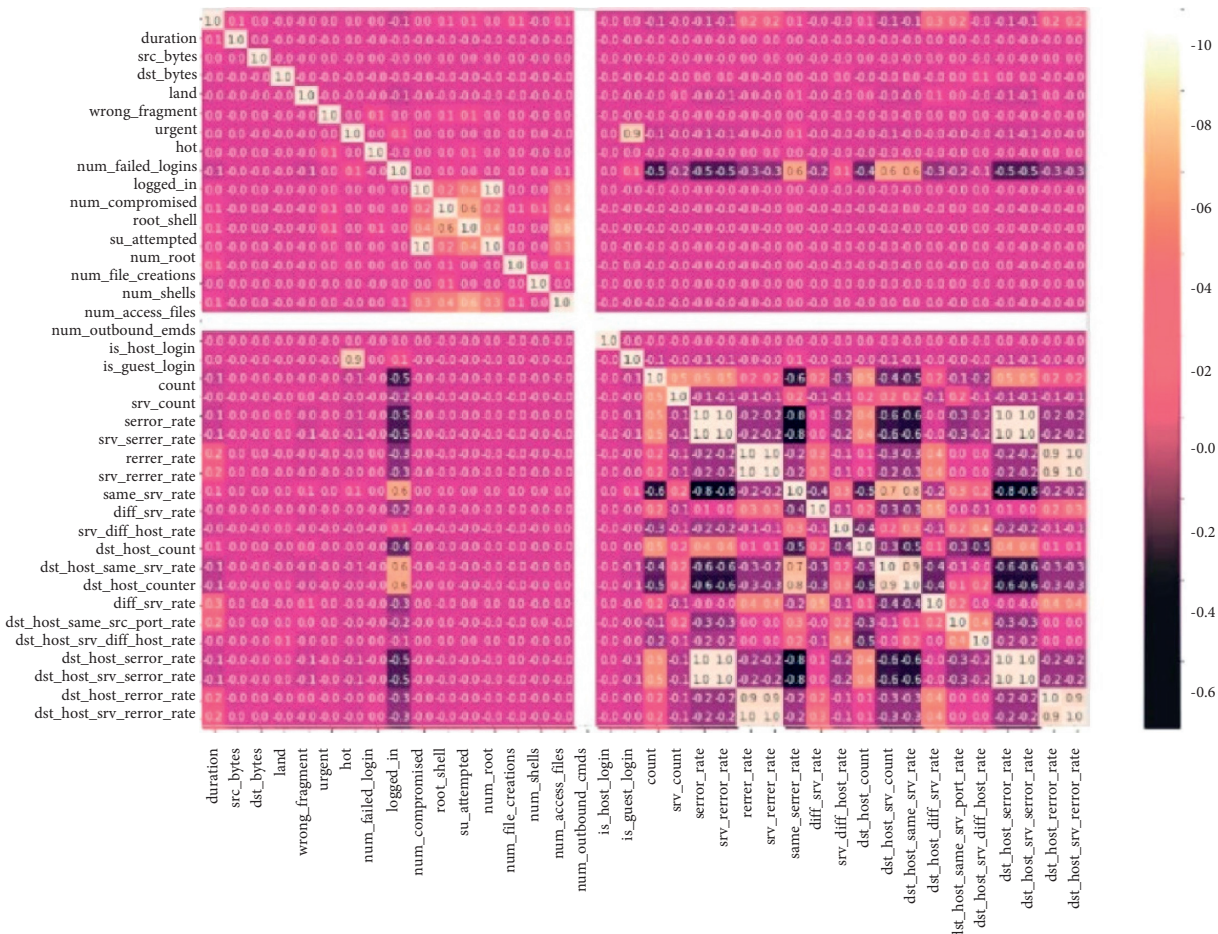

Figure 6: Feature means per class.

data in a single class, using the "binary class" variable that we created earlier.

4.1. Model Evaluation. We have applied Convolutional Neural Networks to the dataset. The following are the results we have gained.

We use the Convolutional Neural Networks decision regression for an intrusion detection method as a special framework (IDS). As we know, in recent studies, CNN has been used by no other researcher in the field of IDS. The CNN decreases the cost function for sparsity classifying IDS. The CNN showed various qualities, such as high graduation precision, detection rate and a training time for a model, and average training duration per sample, which were especially suitable for IDS. Table 4 shows the model training and validation of 1D Convolutional Neural Network (binary classification).

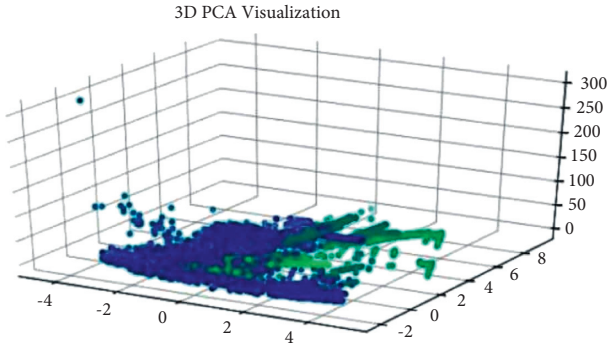

Figure 7: Dimensionality reduction in Feature Engineering.

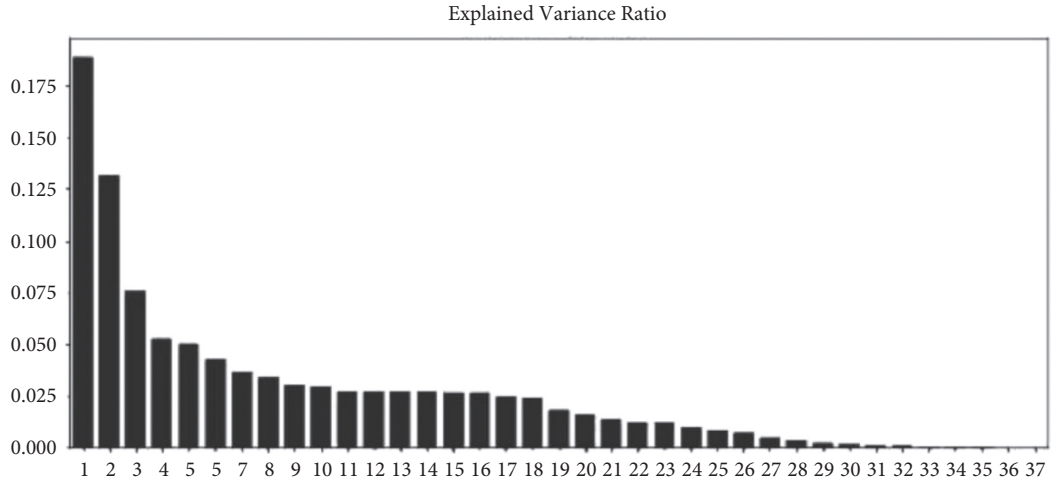

Figure 8: Explained variables ratio.

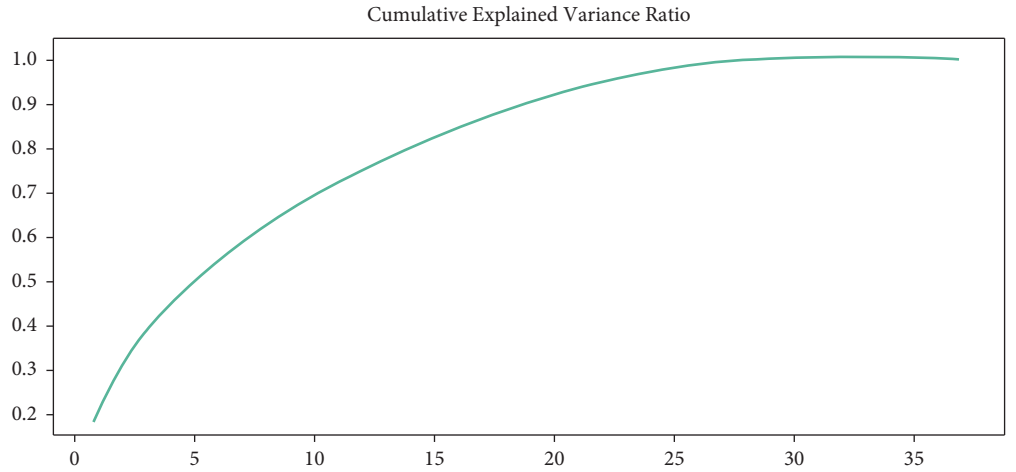

Figure 9: Cumulative variance ratio.

Figure 11 shows the CNN-based binary classification accuracy, precision, recall, and F1 score, which are 99%, 98%, 97%, and 97%, respectively.

Figure 12 shows the CNN-based multiclassification accuracy, precision, recall, and F1 score, which are 98%, 99%, 98%, and 98%, respectively.

We can forecast the future through machine learning and classify the right class. In this research, we employed the new binary and multiclass classification model of Convolutional Neural Networks (CNN) to identify the anomaly of the network system. In this respect, we used the NSLKDD dataset. CNN model has shown the promising results of

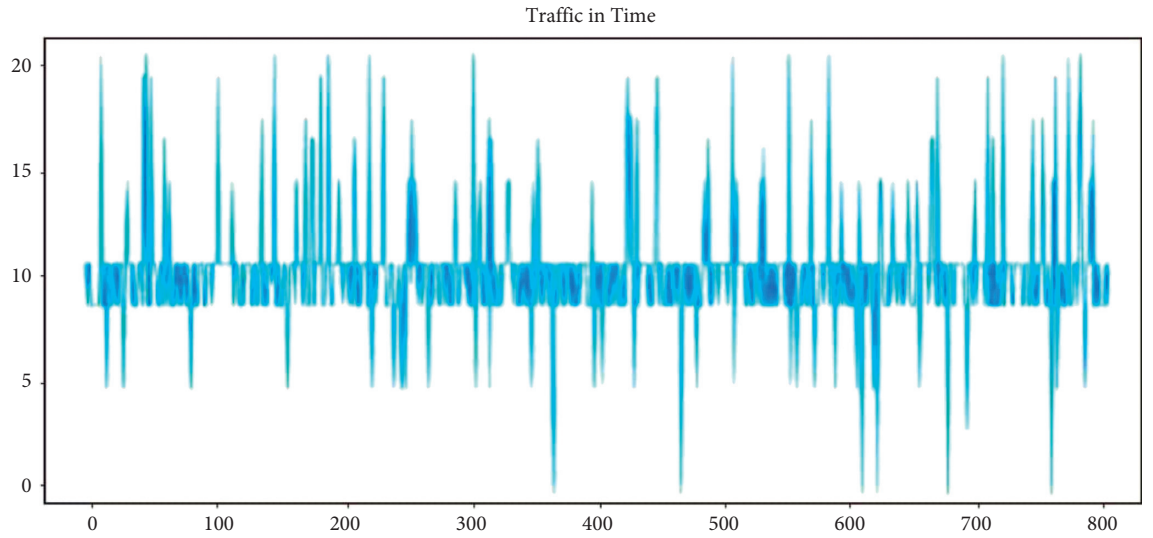

Figure 10: Visualization of Traffic in Time using Label Encoder.

Table 4: Model training and validation of 1D Convolutional Neural Network (binary classification).

Epoch	Accuracy	Loss	Validation accuracy	Validation loss
1	0.91	0.19	0.95	0.03
2	0.92	0.18	0.96	0.03
3	0.93	0.18	0.97	0.03
4	0.94	0.17	0.98	0.023
5	0.97	0.17	0.99	0.021
6	0.98	0.15	0.991	0.002
7	0.992	0.13	0.992	0.0019
8	0.994	0.12	0.993	0.0018
9	0.995	0.12	0.997	0.0017
10	0.995	0.12	0.998	0.0016
11	0.995	0.12	0.998	0.0012

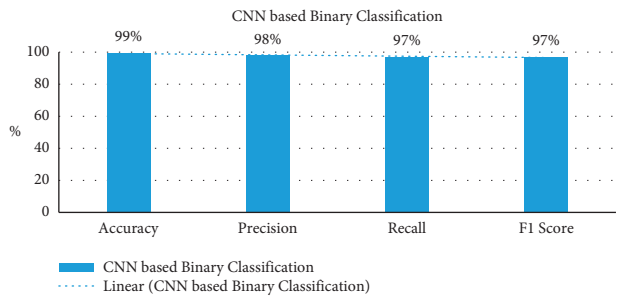

Figure 11: CNN-based binary classification.

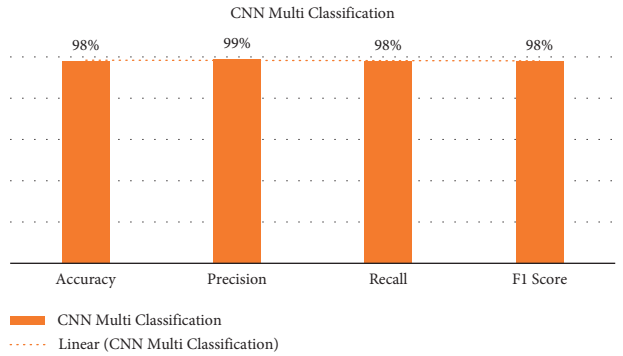

Figure 12: CNN-based multiclassification.

Table 5: Comparison table with the state-of-the-art literature works.

Authors	Techniques	Accuracy (%)	Outcome
Hemalatha et al. [14]	ANN	89	Intrusion
Debar et al. [28]	ANN	87	Anomaly
Yassin et al. [29]	Decision trees	78	Anomaly
Gandhi et al. [30]	Decision trees	89	Anomaly
Our approach	Convolutional Neural Networks	99	Anomaly, outlier, and inlier

multiclass and binary classification in terms of validation loss of 0.0012 at 11th epochs and validation accuracy of 98% and 99%, respectively. Following is the comparison table with the state-of-the-art literature works; Table 5 shows the comparison table with the state-of-the-art literature works.

5. Some Common Mistakes

In the intrusion detection system, the system checks the blockage in the network due to traffic. It will check the firmware and detect the anomaly in the network. If the IDS detects any anomaly, it will send it back to the user. There are two types of threats, that is, active and passive. We have detected both threats using Convolutional Neural Networks, and our system detects the anomaly. The system accuracy is very good as compared to previous researches, and it reaches almost between 90 and 95% of the best possible accuracy. We use the Convolutional Neural Networks decision regression for an intrusion detection method as a special framework (IDS). As we know, in recent studies, CNN has been used by no other researcher in the field of IDS. The CNN reduces the cost function for sparsity classifying IDS. The CNN exhibited a number of characteristics that made it particularly ideal for IDS, including high graduation precision, detection rate, model training time, and average training length per sample. Our research can be carried out using optimization approaches such as particle swarm optimization, grey wolf optimization, and whale optimization techniques, which can improve the results of machine learning models. This implementation can be altered by using feature selection techniques. By using feature selection techniques, we can improve the results of machine learning models.

Data Availability

The dataset used in this paper is available from the author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (Grant no. 662162039), Educational Commission of Gansu Province, China (Grant no. 2017C-05), and Foundation for the Key Research and Development Program of Gansu Province, China (Grant no. 20YF3GA016).

References

[1] J. Lansky, S. Ali, M. Mohammadi et al., "Deep learning-based intrusion detection systems: a systematic review," *IEEE Access*, vol. 9, pp. 101574–101599, 2021.

[2] A. Fragkiadakis, V. Angelakis, and E. Z. Tragos, "Securing cognitive wireless sensor networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 10, no. 3, Article ID 393248, 2014.

[3] Z. Hu, L. Wang, L. Qi, Y. Li, and W. Yang, "A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network," *IEEE Access*, vol. 8, pp. 195741–195751, 2020.

[4] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," *IEEE Access*, vol. 7, pp. 64366–64374, 2019.

[5] C. Yue, L. Wang, D. Wang, R. Duo, and X. Nie, "An ensemble intrusion detection method for train ethernet consist network based on CNN and RNN," *IEEE Access*, vol. 9, pp. 59527–59539, 2021.

[6] A. Kim, M. Park, and D. H. Lee, "AI-IDS: application of deep learning to real-time web intrusion detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020.

[7] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical network," *IEEE Access*, vol. 8, no. 3, pp. 32464–32476, 2020.

[8] H. Park, S. Park, and Y. Joo, "Detection of abandoned and stolen objects based on dual background model and mask R-CNN," *IEEE Access*, vol. 8, pp. 80010–80019, 2020.

[9] Y. Meidan, M. Bohadana, A. Shabtai et al., "Detection of unauthorized IoT devices using machine learning techniques," 2017, http://arxiv.org/abs/1709.04647.

[10] R. U. Khan, X. Zhang, R. Kumar, A. Sharif, N. A. Golilarz, and M. Alazab, "An adaptive multi-layer botnet detection technique using machine learning classifiers," *Applied Sciences*, vol. 9, no. 11, pp. 2375–11, 2019.

[11] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim, and M. Alrashoud, "An efficient spam detection technique for IoT devices using machine learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 903–912, 2021.

[12] K. Kumar Gola, N. Chaurasia, B. Gupta, and D. Singh Niranjan, "Sea lion optimization algorithm based node deployment strategy in underwater acoustic sensor network," *International Journal of Communication Systems*, vol. 34, no. 5, pp. 1–18, 2021.

[13] D. Sahoo, C. Liu, and S. C. H. Hoi, "Malicious URL detection using machine learning," *Surveyor*, vol. 1, no. 1, pp. 1–37, 2017, http://arxiv.org/abs/1701.07179.

[14] A. Hemalatha and Selvabrunda, "Mobile malware detection using anomaly based machine learning classifier techniques," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11S2, pp. 260–267, 2019.

[15] D. Anderson, T. Frivold, and A. Valdes, *Next-generation Intrusion Detection Expert System (NIDES): A Summary*,

Computer Science Laboratory, SRI International, Menlo Park, CA, USA, 1995.

[16] S. Hariri, M. C. Kind, and R. J. Brunner, "Extended Isolation Forest," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 4, 2021.

[17] L. Khan, M. Awad, and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering | SpringerLink," 2020, https://link.springer.com/article/10.1007%2Fs00778-006-0002-5.

[18] D. Endler, "Intrusion detection. Applying machine learning to Solaris audit data," in *Proceedings of the - Annual Computer Security Application Conference ACSAC*, pp. 268–279, Scottsdale, ARI, USA, December 1998.

[19] S. Axelsson, *Research in Intrusion Detection Systems: A Survey*, Chalmers University of Technology, Gothenburg , Sweden, 1999.

[20] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based intelligent intrusion detection system in internet of vehicles," in *Proceedings of the 2019 IEEE Glob. Communications Conference GLOBECOM 2019 - procedings*, Big Island, HW, USA, December 2019.

[21] A. Manimaran, D. Chandramohan, S. G. Shrinivas, and N. Arulkumar, "A comprehensive novel model for network speech anomaly detection system using deep learning approach," *International Journal of Speech Technology*, vol. 23, no. 2, pp. 305–313, 2020.

[22] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.

[23] J. Anitha Ruth, H. Sirmathi, and A. Meenakshi, "Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks," *IET Information Security*, vol. 13, no. 4, pp. 321–329, 2019.

[24] Y. Li, J. Wang, Z.-H. Tian, T.-B. Lu, and C. Young, "Building lightweight intrusion detection system using wrapper-based feature selection mechanisms - ScienceDirect," 2020, https://www.sciencedirect.com/science/article/pii/S0167404809000030?via%3Dihub.

[25] S. O. Al-mamory and F. S. Jassim, "On the designing of two grains levels network intrusion detection system," *Karbala International Journal of Modern Science*, vol. 1, no. 1, pp. 15–25, 2015.

[26] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 14–25, 2021.

[27] A. Liu and B. Sun, "An intrusion detection system based on a quantitative model of interaction mode between ports," *IEEE Access*, vol. 7, pp. 161725–161740, 2019.

[28] M. Dacier, A. Wispe, and H. Debar, "A revised taxonomy for intrusion detection systems," *Annales des Telecommunications*, vol. 55, no. 7/8, pp. 361–378, 2000.

[29] W. Yassin, N. I. Udzir, and Z. Muda, "Anomaly-based intrusion detection through K- means clustering and naive bayes classification,"vol. 049, pp. 298–303, in *Proceedings of the 4th International Conference Computer Informatics*, vol. 049, pp. 298–303, ICOCI, Kuching, Malaysia, August 2013.

[30] S. Srivasta, G. Meera Gandhi, Effective network intrusion detection using classifiers decision trees and decision rules," *International Journal of Advanced Networking and Applications*, vol. 2, no. 3, pp. 686–692, 2010.