Journal of Education for Pure Science
Vol.14, No.1 (2025)
DOI: https://www.doi.org/%2010.32792/jeps.v15i1.505

Website: jceps.utq.edu.iq *Email: jceps@eps.utq.edu.iq*

A hybrid feature learning model to enhance multilayer perceptron for network intrusion detection

Noor Abdulkaadhim Hamad[1,], **Oras Nasef Jasim**[2,] **and Zainab Kashlan Yaser**[*,3,]

[1]General Directorate of Education in Thi-Qar Governorate, Thi-Qar, Iraq
[2]General Directorate of Education in Thi-Qar Governorate, Thi-Qar, Iraq
[3]General Directorate of Education in Thi-Qar Governorate, Thi-Qar, Iraq

[*] Corresponding email: noor_abd@utq.edu.iq

Received 28 /07 /2024, Accepted 14/ 10 /2024, Published 01 / 03 /2025

Abstract:

The rapid advancement of computer and network technologies has led to a surge in network security threats. To combat these risks, Intrusion Detection Systems (IDS) have become essential for detecting and mitigating network attacks. Machine learning-based technologies present interesting possibilities for improving the accuracy and reliability of intrusion detection. However, the effectiveness of these methods might be jeopardized by high-dimensional datasets with irrelevant or duplicated features, which can reduce model performance and lengthen training time. This study takes a multifaceted approach to addressing these difficulties. Firstly, we suggest a data balancing strategy that combines oversampling and undersampling techniques to provide a more balanced dataset, hence improving the detection of both normal and harmful actions. Second, we use dimensionality reduction approaches to select and extract useful features, minimizing the impact of irrelevant data on model performance. Third, we use advanced deep learning techniques to improve the detection accuracy of network intrusions. We evaluate our proposed methodology against the NSL-KDD dataset, a well-known network intrusion detection benchmark. The experimental results show that our methodology enhances intrusion detection accuracy greatly when compared to existing methods. Combining balanced data, feature selection, and advanced deep learning approaches effectively addresses network intrusion detection difficulties, resulting in more reliable and efficient IDS solutions.

Keywords: Class imbalance, Classification, Dimensionality Reduction, Intrusion Detection System, Long Short-Term Memory (LSTM), Random Forest, Sparse Autoencoder.

1-Introduction

The Internet has fully revolutionized the world in transactions of business, info resources, socialization, and communication among others. This has contributed immensely to the economic growth of nations and has widely influenced computer network user's numerical growth. However, usage increment of the internet is inherently bogged with systems security of info that raises in sophistication daily [1]. Cyber security has become vulnerable because of intrusion incidents in computer networks and rapid emergence wide expansion. Improving cyber security's importance has attracted significant attention from industry and academia around the world.[2]

An intrusion detection system (IDS) refers to an efficient security mechanism that controls traffic in the network and avoids damaging needs. IDS study is quickly evolving with machine learning improvement. Methods of traditional machine learning have been increasingly applied in intrusion detection like support vector machine (SVM), decision tree (DT), and random forest (RF). Deep learning, convolutional neural network (CNN), recurrent neural network (RNN), and long short-term memory (LSTM) improvements are becoming well-known in intrusion detection [3]. Such methods are given various rules, and the way that efficiently exploits the merits for addressing IDS functions, particularly fields keeps the open study question. In addition, because of high dimensionality and data complexity, the usual solution is using methods of data preprocessing that may aid in decreasing dimensionality and make investigators able to be able to cope with such high-dimensional spaces. Techniques of Preprocessing could influence the performance of detection which must be carefully taken in intrusion-detection techniques' design.

Recently, different supervised and unsupervised algorithms of machine learning have been utilized to improve the detection of network intrusion performance [4]. Present algorithms of detection have issues presenting good performance. At first, ignore the class imbalance problem and the impact it has on the performance of classification that causes the wide reduction in rates of detection, especially for minority classes. Second, many irrelevant and relevant data overlap in a high-dimensional dataset by grouping the detection of network intrusion. Third, low rate of accuracy. At last, high rate of false alarms. So, the study provides a new model of detection for solving the above issues. The contributions of the proposed method as the following:

- This paper presents a novel technique to solve the issue of the imbalanced dataset. Hybrid sampling methods combine the Neighborhood Cleaning Rule (NCL) to reduce the majority samples and the Support Vector Machine - Synthetic Minority Over-sampling Technique (SVM-SMOTE) to increase the minority samples.
- A hybrid feature learning model is used to reduce the dimensionality, which combines an unsupervised deep learning algorithm followed by the machine learning algorithm. More specifically, we use the power of Sparse Auto-Encoder (SAE) as feature extraction to reduce the high dimensionality of features, then use the speed of RF to select the most important feature .
- Improvement of the detection using a version of the Artificial Neural Network (ANN) algorithm, namely Multi-Layer Perceptron (MLP).
- This paper conducts experiments on the newer and more comprehensive NSL KDD dataset using different evaluation measures such as recall, accuracy, f-measure, and precision, rate of accuracy.

However, this paper provides a new model of detection for solving the above issues. The rest of the paper is as follows: In Section 2, we review the previous work. In Section 3, we present the proposed method. Section 4 discusses the test results, and the final section presents the conclusions of the paper.

2- Related Work

In the last two decades, methods of machine learning (ML) have been widely applied in the field of network security due to the capability for concealed info extraction on distinctions between bad and usual manners [5]. Thus, previous investigators applied different strategies given the conventional ML for intrusion detection (ID). In [6], a convolutional recurrent neural network (CRNN) is applied to making the hybrid ID framework based on DL which predicts and classifies bad cyberattacks in the network. In hybrid CRNNIDS, CNN carries out convolution for getting local features, and recurrent neural network (RNN) gets temporal features for developing performance and prediction of the ID system. However, while this method improved detection accuracy, it suffered from high computational costs.

In [7], shows learning algorithms usage machine for traffic control in bad network manner as part of NIDS in SDN controller. Various classical and developed machine learning methods based on tree, XGBoost, Random Forest, and Decision Tree are selected for showing diagnosis of attack. Though effective for specific attack patterns, these models lacked the adaptability to handle evolving threats in real time.

In [8], applies the hybrid Deep learning method based on optimization for multi-level IDS process. Firstly, the model of fisher score is used for basic feature extraction. After that, in data size, data augmentation is raised. Here, Rider Optimization Algorithm-Based Neural Network (RideNN) is used for the diagnosis of the first level that data is grouped as normal and attacker. The method improved classification but required complex feature extraction processes that may not be suitable for real-time systems.

In [9], a robust and effective intrusion detection technique, known as RV coefficient and Exponential Sea Lion Optimization-enabled Deep Residual Network (ExpSLO-enabled DRN), is developed using Spark. Now, unique features are chosen applying presented RV hybrid feature fusion based on coefficient that is modeled by Canberra distance, wrapper class-wise information gain (CIG) incorporation in slave node. Despite the improved accuracy, the model complexity could hinder scalability in large-scale deployments.

In [10], improves the robust IDS scheme known as Remora Whale Optimization (RWO)-based Hybrid deep model to detect intrusions. Now, input data is pre-processed, then data is transformed. Using transformed data, efficient CNN features are extracted and feature conversion is carried out to transform features in vector shape. While effective in reducing false positives, the feature transformation process added unnecessary complexity to the model.

In [11], offers the model for traffic unusuality diagnosis known as the deep learning model for network intrusion detection (DLNID) that integrates the attention mechanism and bidirectional long short-term memory (Bi-LSTM) network, firstly it extracts data traffic order features via CNN network, after that again determines every channel weights via attention mechanism, at last, applies Bi-LSTM for learning order features network. However, this model is often constrained by dataset-specific performance and lacks generalizability.

In [12], for bad activities optimization diagnosis performance in traffic of network, 4 hybrid IDSs are offered for satellite-terrestrial communication systems (SAT-IDSs) here. Whole presented systems exploit the sequential forward feature selection (SFS) technique given the random forest (RF) for choosing essential features from the set of data which raise relevance and decrease complexity and integrate them with machine learning (ML)/deep learning (DL) scheme. However, this model is often constrained by dataset-specific performance and lacks generalizability.

In [13], the hybrid DL scheme and shallow learning are presented for IoT device intrusion detection. The presented scheme firstly applies a spider monkey optimization feature selection algorithm that looks for the most essential features, after that Siamese neural network-based scheme is presented for making data more classifiable. This paper introduces more complexity to the SMO and Siamese network, which may not be ideal for larger datasets or non-IoT systems.

In [14], focuses on enhancing network security through the implementation and evaluation of an intrusion detection system (IDS) based on deep neural networks (DNNs). It explores modern techniques aimed at improving the performance of intrusion detection, recognizing the critical importance of protecting computer networks from malicious activities. This paper focuses mainly on the DNN model itself without addressing the challenges posed by unbalanced or noisy datasets.

In [15], proposes new deep learning architectures with various feature fusion strategies to enhance NIDS multiclassification performance. They present three deep learning models: early-fusion, late-fusion, and late-ensemble. These models use feature fusion and fully connected deep networks. The feature fusion technique improves the model's ability to learn relationships between input features. However, the complexity of this approach may limit its real-time application.

3- Proposed method

In the first phase, we present the data-level technique which integrates techniques of over-sampling and under-sampling for solving imbalanced data. After that, we integrate algorithms of deep learning and machine learning to decrease high dimensional, eliminating redundant and irrelevant basic features. At last, we apply the algorithm of deep learning for classification.

Flowchart contains four steps (1) Pre-processing of Data (2) Balancing dataset (3) reduction of Dimensionality (4) Classification. The steps are illustrated in Figure 1.

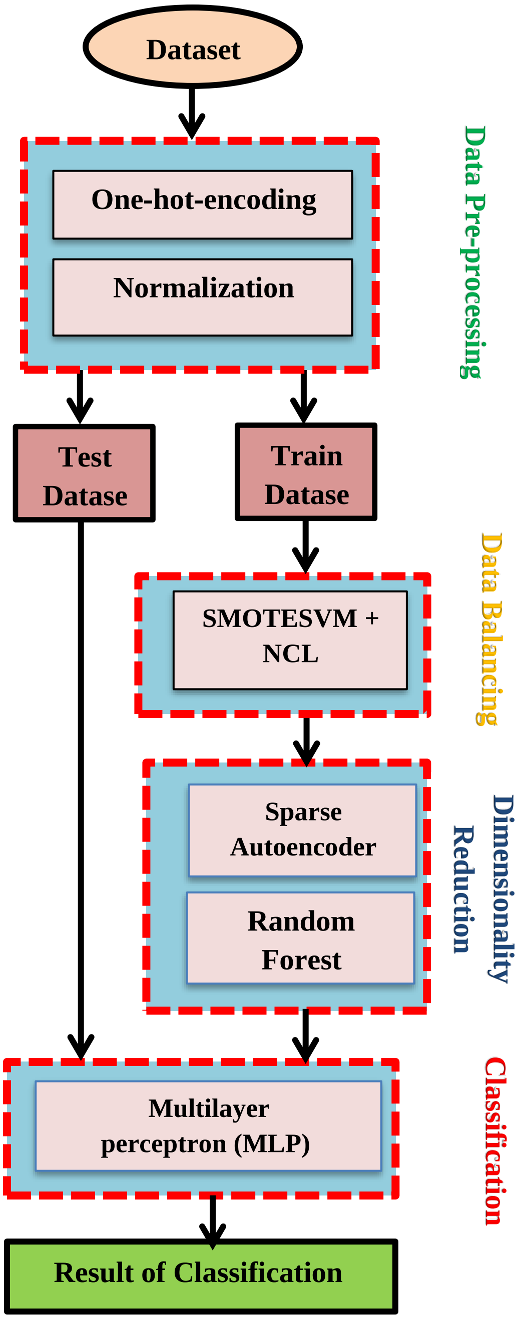

Figure 1. Flowchart of the proposed method

Pre-processing of Data: this is important for network intrusion detection. This contains normalization and one-hot encoding.

- One-hot-encoding: this is the most well-known technique to cope with categorical attribute neutralization due to that this is an effective and simple method of encoding [12]. Each categorical value of an attribute can be converted to the binary vector that just only has one component with value 1, as well as the whole others, are zeros. Component by value 1 shows the corresponding possible value categorical attribute presence.
- Normalization: here, the technology of min-max normalization [13] reduces various dimensional scales. Basic data is transformed linearly before being scaled to [0,1]. The equation below utilizes min-max values for conducting the conversion of data.

$$z(i) = \frac{x_i - \min(x)}{\max(x) - \min(x)} \qquad (1)$$

That z(i) shows the normalized value, xi refers to the related value of the attribute, and min(x) and max(x) are respectively minimum and maximum attribute values.

Balancing dataset: here, the level approach of data (an approach based on sampling) is utilized for controlling imbalanced issues of data. The Approach of data level is one of the most common methods that can solve the imbalanced issues of data. The approach has the target of establishing a balanced dataset of training with preprocessing data via artificial manipulation. three data-level approach groups exist, including Hybrid-Sampling [17], Under-Sampling, and Over-Sampling [16].

- Under-sampling: this is the non-heuristic strategy that chooses the majority class subset for creating the balanced distribution of class.
- Over-sampling: this is the non-heuristic strategy for balancing the distribution of class, thus duplicating the minority class samples.
- Hybrid-sampling: under-sampling and over-sampling strategies combination. The strategy removes objects from the majority class and creates objects for the minority class.

Here, we utilize methods of hybrid–sampling for solving imbalance classes that integrate SVM-SMOTE as Over-sampling and Neighborhood Cleaning Rule (NCL) as under-sampling.

The Neighbourhood Cleaning Rule (NCL) [18] modifies the Edited Nearest Neighbor Rule (ENN) [19]. NCL is the technique for improving majority class instance data cleanliness. NCL remains between the methods of undersampling due to this consideration of data quality to be removed. This is not concentrating just on the reduction of data but also cleaning of data.

SVM-SMOTE [20] develops SMOTE that creates novel instances of minority classes close to borderline applying the model of SVM for assisting boundaries set among majority and minority classes [21].

Reduction of Dimensionality: the study concentrates on the extraction and selection of features for decreasing dimensions as well as eliminating unwanted features.

- Extraction of Features: this is the technique for building novel features that are related to the basic input set for reducing high feature vector dimensionality. The paper utilizes a sparse autoencoder (SAE) [22] for decreasing unlabeled and high-dimensional basic data.
- Selection of Feature: this plays an essential role in improving disease detection by fewer features. three basic methods of feature selection exist which are, embedded, filter, and wrapper [23]. The embedded method integrates both filter and wrapper methods' advantages [24]. One of the embedded methods groups is random forest. The study is according to the method of embedded which utilizes the algorithm of random forest in the selection of features. The random forest has objectives below in the selection of features including: (1) Random features selection, as well as data, can develop the performance of classification and (2) Low overfitting. (3) Easy interpretability.

Classification: applying the strategy of deep learning according to MLP for detecting the NSLKDD dataset normal and attack groups.

4- Discussion and Experiments

The datasets utilized, implementation, also proposed method results are discussed in this part. In this section, the obtained results for the proposed method are discussed.

Firstly, the dataset utilized in the research will be defined and present variables will be described one by one.

4.1 Performance Measures

The novel proposed method has been done in Python. This paper evaluated our proposed model using different performance measures to determine its effectiveness. The metrics are specified as follows:

Table 1. Table of the confusion matrix.

Predicted class label			
attack	normal	Predicted/real	
False positive (FP)	True negative (TN)	normal	**Real class label**
True positive (TP)	False negative (FN)	attack	

- **True positive**: samples that are diagnosed accurately by test as an attack.
- **False positive**: samples that are diagnosed wrongly by test as an attack.
- **True negative**: samples that are diagnosed accurately by test as normal.
- **False negative**: samples that are diagnosed wrongly by test as normal.

Confusion matrix diagonal provides appropriate predictions, while non-diagonal components provide inappropriate specific classifier predictions. Such confusion matrix features are illustrated in Table 1. So, the measures of assessment below have been used in recent articles.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \qquad (2)$$

$$Recall\ or\ Detection\ Rate = \frac{\text{TP}}{\text{TP+FN}} \qquad (3)$$

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \qquad (4)$$

$$\text{F-Measure} = 2 \times (\frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}}) \qquad (5)$$

4.2 Results evaluation

After performing a proposed method in the environment of Python, we compared the proposed method as well as other methods on datasets. We assign data classification percentages to train and test equal to 80 and 20.
Table 2 provides a comparison for accuracy for classifying the two classes for the proposed method and the other articles. To classify two classes, tuples are described as healthy and patient classes. The accuracy for the proposed method and other methods in [8,9,14,15] was 98%, 93.8%, 90.73%, 86.81%, and 94.38% respectively, which has improved by 4.2% compared to the method [8]. Compared with the method [9], the accuracy of the proposed method achieved 98% and 90.73%, respectively, which has improved by 7.27% compared to the method [9]. Compared with the method [14], the accuracy of the proposed method achieved 98% and 86.81%, respectively, which has improved by 11.10% compared to the method [14]. Compared with the method [15], the accuracy of the proposed method achieved 98% and 94.38%, respectively, which has improved by 3.62% compared to the method [15]. The performance measures are under the accuracy of each classification algorithm. Among the three classification algorithms used, the highest accuracy has been observed in the proposed method and the results show that the proposed method is the best. Figure 2 shows the comparison of the accuracy of the proposed method and other methods.

Table 2. Results of comparison of the proposed method and other methods

Methods	Accuracy	Recall	Precision	F-Measure
In [8]	93.8%	93.2%	92%	92.6%
In [9]	90.73%	93.17%	86.38%	89.65%
In [14]	86.81%	86.80%	86.86%	-
In [15]	94.38%	94.22%	94.82%	94.34%

Proposed Method	98%	98.11%	97.14%	97.62%

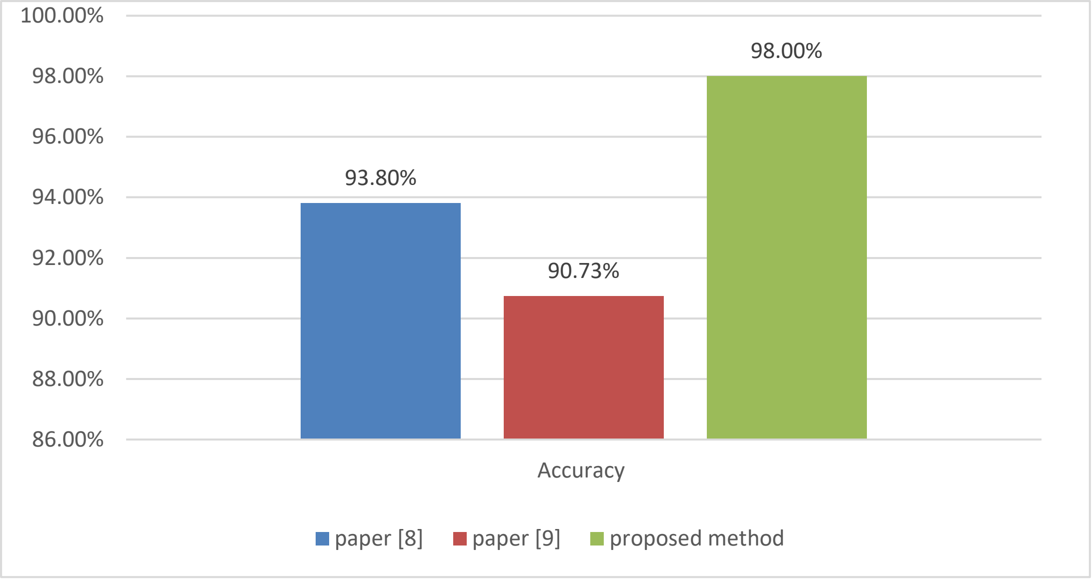

Figure 2. Comparison of accuracy of the proposed method and other methods

The heatmap in Figure 3 illustrates the confusion matrix percent and amounts. Usual traffic percent is grouped since the attack is in FP by SVM, and KNN, possesses similar outcomes. Attack traffic prediction was better in RF across the other mechanisms. Furthermore, as usual, the attack traffic diagnosis percentage was lower in RF than in other techniques.

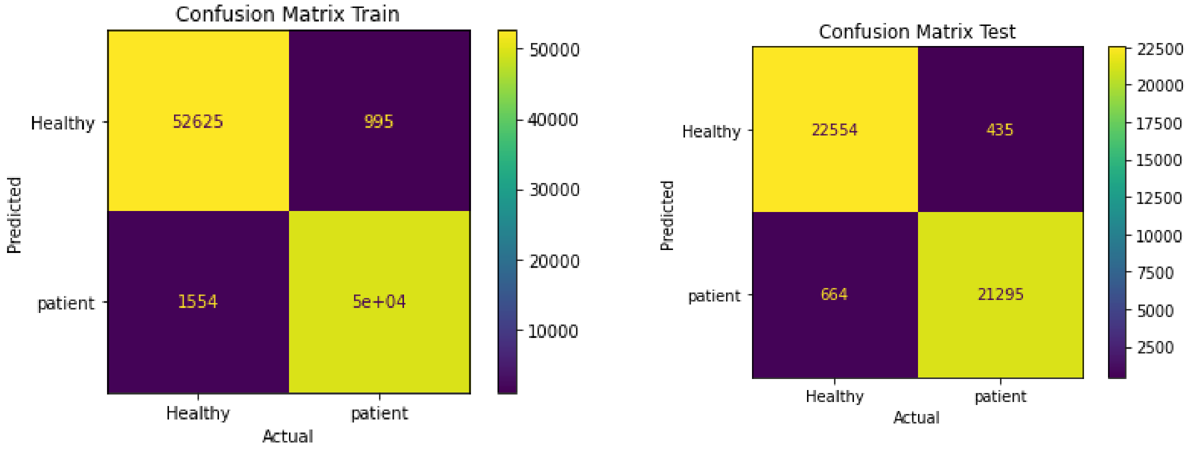

Figure 3. Heatmap of the confusion matrix.

Given the matrix of confusion, different parameters like accuracy are computed. For assessing the presented technique, accuracy is computed for every instance. For presenting total accuracy in various patterns, middle accuracy could be computed by gathering every instance accuracy and sharing outcomes through the sum instances' amount.

The receiver operating characteristics (ROC) curve for the proposed algorithm is shown in Figure 4. The ROC represents the performance of the proposed algorithm concerning true positive and false positive rates, the proposed algorithm gave a ROC of 0.98 in the NSLKDD dataset.

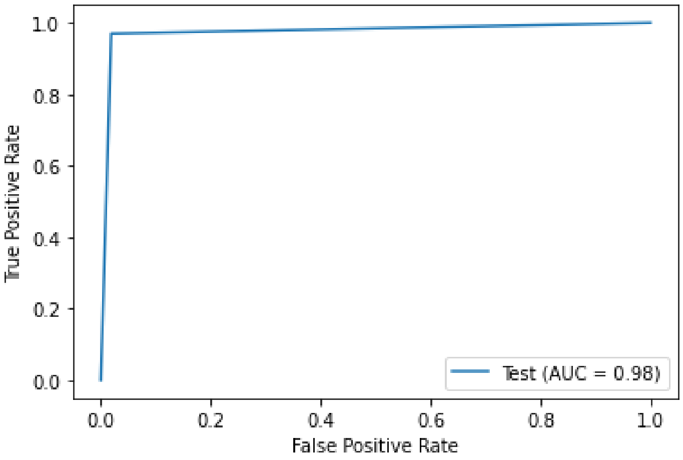

Figure 4. The ROCcurve for the proposeded method

6- Conclusion

Machine learning approach in data analysis provides a wide range of methods that researchers who investigate in various fields begin to use. These applications indicate that supervised learning cannot only be considered as a flexible alternative for parametric regression but also as a powerful prediction method that can be used to target interventions, which is naturally in line with the idea of compatible designs. In today's global classification, it is an important method in data mining, which is used for convolutional neural networks to classify data. In this paper, we have proposed a new model of detection for the prediction of network intrusion. Comparative analysis has been done with existing methods. The performance of the proposed method is tested on the NSLKDD dataset. Accuracy is 98% on the NSLKDD dataset, which is better than existing techniques. This study is hoped to be a reference for doctors when making a diagnosis. For future research, a larger dataset is recommended to get better results.

Conflicts Of Interest

The authors declare no conflicts of interest.

Funding

The authors received no financial support for this research.

References

[1] J. O. Mebawondu, O. D. Alowolodu, J. O. Mebawondu, and A. O. Adetunmbi, "Network intrusion detection system using supervised learning paradigm," *Scientific African*, vol. 9, p. e00497, 2020.

[2] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, p. 107247, 2020.

[3] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, and H. Han, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Computers & Security*, vol. 116, p. 102675, 2022.

[4] M. H. Kadhim and F. Mardukhi, "A Novel IoT Application Recommendation System Using Metaheuristic Multi-Criteria Analysis," *Computer Systems Science & Engineering*, vol. 37, no. 2, 2021.

[5] L. Zolfagharipour, M. H. Kadhim, and T. H. Mandeel, "Enhance the Security of Access to IoT-based Equipment in Fog," in *Proc. 2023 Al-Sadiq Int. Conf. on Communication and Information Technology (AICCIT)*, pp. 142-146, IEEE, 2023.

[6] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," *Processes*, vol. 9, no. 5, p. 834, 2021.

[7] A. O. Alzahrani and M. J. F. Alenazi, "Designing a network intrusion detection system based on machine learning for software-defined networks," *Future Internet*, vol. 13, no. 5, p. 111, 2021.

[8] E. S. GSR, M. Azees, C. R. Vinodkumar, and G. Parthasarathy, "Hybrid optimization enabled deep learning technique for multi-level intrusion detection," *Advances in Engineering Software*, vol. 173, p. 103197, 2022.

[9] M. P. Ramkumar, P. V. B. Reddy, J. T. Thirukrishna, and C. Vidyadhari, "Intrusion detection in big data using hybrid feature fusion and optimization enabled deep learning based on spark architecture," *Computers & Security*, vol. 116, p. 102668, 2022.

[10] S. V. Pingale and S. R. Sutar, "Remora whale optimization-based hybrid deep learning for network intrusion detection using CNN features," *Expert Systems with Applications*, vol. 210, p. 118476, 2022.

[11] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, "A deep learning model for network intrusion detection with imbalanced data," *Electronics*, vol. 11, no. 6, p. 898, 2022.

[12] A. T. Azar, E. Shehab, A. M. Mattar, I. A. Hameed, and S. A. Elsaid, "Deep Learning Based Hybrid Intrusion Detection Systems to protect Satellite Networks," *J. Netw. Syst. Manage.*, vol. 31, no. 4, p. 82, 2023.

[13] S. Hosseini and S. R. Sardo, "Network intrusion detection based on deep learning method in the internet of things," *J. Reliable Intell. Environ.*, vol. 9, no. 2, pp. 147-159, 2023.

[14] F. S. Alrayes, M. Zakariah, S. U. Amin, Z. I. Khan, and J. S. Alqurni, "Network Security Enhanced with Deep Neural Network-Based Intrusion Detection System," *Computers, Materials & Continua*, vol. 80, no. 1, 2024.

[15] A. Ayantayo, A. Kaur, A. Kour, X. Schmoor, F. Shah, I. Vickers, P. Kearney, and M. M. Abdelsamea, "Network intrusion detection using feature fusion with deep learning," *J. Big Data*, vol. 10, no. 1, p. 167, 2023.

[16] B. Duan, L. Han, Z. Gou, Y. Yang, and S. Chen, "Clustering Mixed Data Based on Density Peaks and Stacked Denoising Autoencoders," *Symmetry*, vol. 11, no. 2, p. 163, 2019.

[17] N. Khare, P. Devan, C. L. Chowdhary, S. Bhattacharya, G. Singh, S. Singh, and B. Yoon, "SMO-DNN: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection," *Electronics*, vol. 9, no. 4, p. 692, 2020.

[18] B. W. Yap, K. A. Rani, H. A. A. Rahman, S. Fong, Z. Khairudin, and N. N. Abdullah, "An application of oversampling, undersampling, bagging and boosting in handling imbalanced datasets," in *Proc. 1st Int. Conf. Adv. Data Inf. Eng. (DaEng-2013)*, Springer, Singapore, pp. 13-22, 2014.

[19] M. Galar, A. Fernandez, E. Barrenechea, H. Bustince, and F. Herrera, "A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid-based approaches," *IEEE Trans. Syst., Man, Cybern., Part C (Appl. Rev.)*, vol. 42, no. 4, pp. 463-484, 2011.

[20] J. Laurikkala, "Improving identification of difficult small classes by balancing class distribution," in *Conf. Artif. Intell. Med. Eur.*, Springer, Berlin, Heidelberg, pp. 63-66, 2001.

[21] D. L. Wilson, "Asymptotic properties of nearest neighbor rules using edited data," *IEEE Trans. Syst., Man, Cybern.*, vol. 3, pp. 408-421, 1972.

[22] H. M. Nguyen, E. W. Cooper, and K. Kamei, "Borderline over-sampling for imbalanced data classification," *Int. J. Knowl. Eng. Soft Data Paradigms*, vol. 3, no. 1, pp. 4-21, 2011.

[23] Y. Tang, Y.-Q. Zhang, N. V. Chawla, and S. Krasser, "SVMs modeling for highly imbalanced classification," *IEEE Trans. Syst., Man, Cybern., Part B (Cybernetics)*, vol. 39, no. 1, pp. 281-288, 2008.

[24] A. Ng, "Sparse autoencoder," *CS294A Lecture Notes*, vol. 72, pp. 1-19, 2011.