Article

Application of Deep Learning-Based Intrusion Detection System (IDS) in Network Anomaly Traffic Detection

Fanyi Zhao *, Hanzhe Li, Kaiyi Niu, Jiatu Shi, Runze Song

Posted Date: 8 July 2024

doi: 10.20944/preprints202407.0595.v1

Keywords: Deep learning; Intrusion detection System (IDS); CNN-Focal Model; Abnormal network traffic

Article

Application of Deep Learning-Based Intrusion Detection System (IDS) in Network Anomaly Traffic Detection

Fanyi Zhao [1,*], Hanzhe Li [2], Kaiyi Niu [3], Jiatu Shi [4] and Runze Song [5]

[1] Computer Science, Stevens Institute of Technology, NJ, USA
[2] Computer Engineering, New York University, New York, USA
[3] Artificial intelligence, Royal Holloway University of London, Egham, UK
[4] Computer Science, University of Electronic Science and Technology of China, Cheng Du, China
[5] Information System & Technology Data Analytics, California State University, CA, USA
* Correspondence: fzhao12@stevens.edu

Abstract: This study discusses the application of deep learning technology in network intrusion detection systems (IDS) and focuses on a new model named CNN-Focal. First, through the review of traditional IDS technology, it analyzes its limitations in dealing with complex network traffic. Then, the design principle of the CNN-Focal model is described in detail, which uses threshold convolution and SoftMax multi-class classification technology to effectively improve abnormal traffic detection's accuracy and efficiency. The experimental results show that CNN-Focal performs well on the open data set, demonstrating the potential and advantages of its application in the natural network environment and providing a new perspective and method for further research of deep learning in the field of network security in the future.

Keywords: deep learning; Intrusion detection System (IDS); CNN-focal model; abnormal network traffic

1. Introduction

In the digital age, network intrusion detection is essential in ensuring network security. With the popularization of networks and the interconnection of information, network intrusion events occur frequently, which bring severe threats and losses to countries, organizations, and individuals. Therefore, it is an urgent task to develop an efficient and reliable network intrusion detection system. Network intrusion is a kind of behavior that causes threats and harm to network systems, including unauthorized access, malware attacks, denial of service attacks, and so on. To protect the security of network systems, network intrusion detection becomes an important task. Traditional network intrusion detection methods are usually based on rules and statistical models, but these methods are limited by the accuracy of rules and the generalization ability of models [1]. In recent years, the development of deep learning technology has provided new opportunities for network intrusion detection. Network intrusion detection is a critical problem in the field of network security. Many researchers and scholars have proposed various methods and techniques to detect and prevent network intrusion. Over the past few decades, researchers have come up with several rule - and feature-engineering-based approaches that rely primarily on artificially defined regulations and features to detect intrusion behavior. However, due to the complexity and diversity of network intrusions, these methods often need help to meet the accuracy and efficiency requirements. In recent years, deep learning-based methods have made significant progress in the field of network intrusion detection [2,3]. Deep learning is a branch of machine learning that simulates the learning and decision-making processes of the human brain by building multi-layered neural networks. Compared to traditional methods, deep learning can automatically learn features and patterns from raw data without relying on manually designed rules and features. This makes deep learning more adaptable and accurate in network intrusion detection.

Network intrusion detection methods based on deep learning can be divided into anomaly detection and classification-based methods. The method based on anomaly detection detects and identifies abnormal behaviors that are inconsistent with normal behaviors by building a model of regular network traffic. These methods mainly use autoencoders, variational autoencoders, generative adversarial networks, and other models to learn the distribution of regular network traffic [4]. The classification-based approach turns the network intrusion detection problem into a binary classification problem by training neural networks to distinguish between regular traffic and intrusion behavior. These methods mainly use convolutional neural networks, recurrent neural networks, attention mechanisms, and other models to learn features and patterns.

2. Related Work

2.1. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) originated from a "computer security threat monitoring and surveillance system" proposed by Anderson et al. [5] in 1980 for processing user audit data. Based on the same principle, Denning proposed to use the user characteristics generated by audit data to identify intrusions, that is, to obtain knowledge of the subject's behavior relative to the object's behavior from audit records and rules for detecting abnormal behavior. These pioneering works define the concepts related to intrusion detection. As a network security protection technology, IDS can make full use of software and hardware to detect malicious activities by monitoring a network or system and issuing alerts in time to provide managers with responsive decisions, thus ensuring the confidentiality, integrity, and availability of network resources.

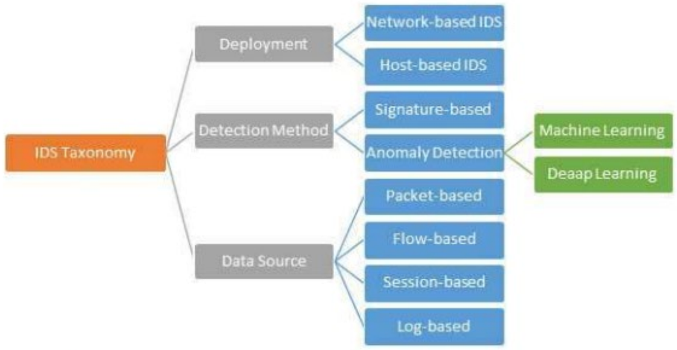

Figure 1. IDS classification.

Intrusion detection technology has played an essential role in the task of network security protection. With the development of machine learning, there has been much research on the application of related technologies in intrusion detection. However, with the continuous escalation of attacks and the rapid growth of network data volume, coupled with the emergence of insider threats, zero-day vulnerabilities, encryption attacks, and other behaviors in recent years, IDS based on traditional machine learning methods has made it difficult to cope with these new challenges [6,7]. Deep learning is a kind of machine learning that can learn the inherent laws of sample data and is more efficient in feature extraction and model building, which is very suitable for current cyber-attack detection.

In this paper, through sorting out the relevant work of intrusion detection, first briefly introduced the latest research on intrusion detection using machine learning methods, then discussed the intrusion detection technology based on deep learning in detail, and finally discussed the existing problems and future development direction

2.2. Classification of Intrusion Detection Systems

1. Classification based on data source

According to the different sources of detected data, intrusion detection can be divided into host-based intrusion detection and network-based intrusion detection.

Host-based intrusion detection (HIDS) [8] collects input data from the hosts monitored by HIDS. Generally, HIDS uses log files as their primary information source and effectively identifies various intrusions by decoding and analyzing log files. The advantages of HIDS are its high-cost performance and low false positive rate. Still, the disadvantages are that only specific programs on the host can be monitored, they need to be installed on each host, and the detection range is limited.

Network-based Intrusion detection (NIDS) [9] detects Network packets and analyzes the contents of packets to determine whether there are attacks in the network. With the widespread use of the Internet, IDS has focused on attacks on the network itself. The advantage of NIDS is that it can monitor the entire network through a system without installing software on each host. The disadvantage is that its detection range is generally limited to the non-encrypted information in transmission, and it is challenging to realize the detection that requires a large amount of computation and an extended analysis time.

2. Classification based on detection technology

Specific to the detection methods used, the field of intrusion detection mainly includes misuse-based intrusion detection and anomaly-based intrusion detection.

Misuse-based Intrusion detection (MIDS) matches network traffic with the existing attack signature database and determines the intrusion behavior based on the matching. The premise is that there is a way to represent the attack, such as in the form of a pattern or signature.

Anomaly-based intrusion detection (AIDS) usually requires the recording of everyday activities in the system, determining the characteristics of these activities, and quantitative description; when the user behavior deviates from the regular record, these behavior activities are defined as attacks. Anomaly-based IDS can detect unknown attacks, so it is the focus of scholars' research.

2.3. Intrusion Detection Technology of Traditional Machine Learning

Traditional machine learning methods have been widely used in anomaly-based intrusion detection. Generally, machine learning can be divided into supervised learning, unsupervised learning, and semi-supervised learning [10]. This section introduces it from three aspects according to this classification standard, and finally, it summarises and analyses the shortcomings of intrusion detection based on traditional machine learning methods.

1. Oversee machine learning methods

(1) Hidden Markov model

Hidden Markov Models (HMM) are probabilistic models about timing, which can be applied to sequential correlation problems in intrusion detection. For the security of Web applications, [11] represented the payload as a byte sequence and analyzed it using the Hidden Markov Model (HMM). After experimental evaluation, the method was particularly effective against the most common Web application attacks (such as XSS and SQL injection). Still, the process needed to consider the length of the payload. There is scope to improve overall accuracy further. [12] applied HMM to network intrusion detection based on abnormal traffic, took the traffic feature extracted based on principal component analysis (PCA) as the input value of HMM, and determined the type of traffic according to the output probability. Aiming at the problems of high detection cost and long detection time of intrusion detection systems in vehicle-mounted AD hoc networks, [13] proposed an HMM-based filtering model for intrusion detection systems. This method modeled the state mode of each vehicle in the AD hoc network as HMM to realize fast filtering of messages from vehicles. The intrusion detection system performs well in terms of detection rate, detection time, and detection cost.

(2) K nearest neighbor algorithm

K-Nearest Neighbor (KNN) algorithm has high precision and mature theory, which can solve the multi-classification problem in intrusion detection. With the increase of the feature dimension of network data, the classification performance of the K-nearest neighbor algorithm will be significantly reduced. To solve this problem, [14] used the tree seed algorithm (TSA) to process the original data. After extracting compelling features, KNN was used for classification. Improve the accuracy and efficiency of network intrusion detection. PKNN is an improved version of classical KNN, which is suitable for solving multi-label classification problems. It gives priority to classes that are closer to the samples and the input items to be classified. [15–17] designed a hybrid intrusion detection system that can be applied in real time and is suitable for solving multi-classification problems. Firstly, a naive basis feature selection (NBFS) technique is used to reduce the dimensionality of the sample data. The outliers are eliminated by an optimized support vector machine (OSVM), and finally, PKNN is used to detect the attack. The experimental results on KD99, NSL-KDD, and Kyoto2006+ data sets show that this system can detect attacks quickly and can be used for real-time intrusion detection.

(3) Support vector machine

Support Vector Machine (SVM) is usually used to solve problems such as small samples, nonlinear and high dimensions. It has strong generalization ability and is widely used in the field of intrusion detection. The dimensionality reduction of data in the data sampling stage can significantly improve the detection efficiency. [18] proposed an SVM intrusion detection model based on compressed sampling, which uses the compressed sampling method in the compressed sensing theory to compress the features of network data streams and then uses SVM to classify the compression results. The proposed method significantly reduces the training time and detection time. [19] proposed an SVM attack detection method based on principal component analysis. The original data set was dimensionally reduced by principal component analysis to obtain a principal component attribute set that could improve the classification effect. Then, the SVM classifier was trained using this attribute set. Experiments on the KDD-99 data set showed that this method considerably shortened the detection time and improved the detection efficiency. [20] used logarithms of the marginal density ratios (LMDRT) to process the original features to improve the quality of features, and then constructed SVM-based IDS. Experimental results on the NSL-KDD dataset show that the proposed method has better performance and robustness in accuracy, detection rate, false positive rate, and training speed

2. Unsupervised machine learning methods

Unsupervised learning mainly deals with the problems in such scenarios as lack of prior knowledge, difficulty in manually labeling categories, or high cost through manual labeling. In the field of intrusion detection, unsupervised learning technology does not need to label data categories but can directly classify network data. In addition, unsupervised methods for dimensionality reduction can effectively solve the redundancy and irrelevance problems of data sets. Reduce computing overhead. Standard unsupervised machine learning methods include k-means, Gaussian mixture model, and principal component analysis.

(1) k-means

K-means is a classical Unsupervised Clustering algorithm that is widely used in the field of intrusion detection. K-means can be combined with other methods to improve performance further, and many studies have been done to improve the traditional K-means. [21] combined k-means and classification regression tree (CART) algorithm to construct an intrusion detection model and studied the performance of the hybrid method. [22] proposed a multi-level intrusion detection model to reduce the training time of the classifier and improve its performance. Firstly, the original training data set was optimized by enhancing the k-means algorithm to reduce the training time of the classifier, and then support vector machine. Extreme learning machines were used for multi-level classification. According to the evaluation of the KDD 99 dataset, the ACC index of the model reaches 95.75%.

(2) Gaussian mixture model

The Gaussian Mixture Model [23] (GMM) models the probability distribution of features so it can identify malicious data samples in network traffic. When the distribution of attack samples and standard samples is similar, the Gaussian mixture model can be used to build a model at the feature level to distinguish the two types of samples [24]. To solve the problems of unbalanced training data, high false positive rate, and undetected unknown attacks, [25] used the Gaussian mixture model method to learn the statistical characteristics of each traffic category and used the adaptive threshold technology based on the interquartile space to identify outliers. The evaluation results on the CICIDS2017 dataset show that this method can effectively detect unknown attacks.

(3) Principal component analysis

Principal component analysis (PCA) is a commonly used feature extraction method, which can reduce the dimensionality of high-dimensional data and shorten the training time of the model, so it is widely used in intrusion detection. In literature [26], PCA and Fisher discriminant ratio (FDR) were used for feature selection and de-noising. Then, Probabilistic Self-Organizing Maps (PSOM) were used to model the feature space, which could effectively distinguish between normal and abnormal connections.

2.4. Application of Deep Learning in Intrusion Detection Systems (IDS)

The application of deep learning in intrusion detection systems (IDS) is one of the essential development directions in the field of network security in recent years. Traditional IDS methods rely primarily on rules and statistical models, which, while effective in specific scenarios, often show limitations in the face of increasingly complex and diverse cyber threats. By constructing multi-layer neural networks, deep learning can automatically learn features and patterns from raw data, thus improving the accuracy and efficiency of the IDS system to detect abnormal network traffic. First, the successful application of convolutional neural network (CNN) [27] in network traffic analysis. For example, a company uses CNN-based IDS systems to monitor its internal network traffic. This system can train the CNN model to automatically learn the characteristics of regular traffic and detect any abnormal traffic that is significantly different from the typical pattern. In this way, the system can accurately identify various types of network attacks, such as DDoS attacks or malware spread, so that timely defensive measures can be taken to protect network security.

Secondly, the application of recurrent neural networks (RNNs) and extended short-term memory networks (LSTM) in the field of network security has also shown remarkable results. For example, a financial institution uses an LSTM-based IDS [28] system to monitor its trading system. The system is capable of analyzing transaction data streams in real-time to identify potential fraud or unusual trading patterns. Through continuous training and optimization, LSTM can adapt to changing attack patterns and new threats to ensure the security and integrity of financial transactions.

Finally, the innovative application of generative adversarial network (GAN) [29] in network security. A research team has developed a GAN-based IDS [30] system for simulating and countering the behavior of cyber attackers. By training the generator and discriminator network, the system can generate highly realistic fake data to deceive the attacker and improve the anti-jamming ability of the system. At the same time, the discriminator network can detect unusual behavior patterns when the attacker tries to invade the system so as tt the attacker and respond in time.

Through these practical cases, the application of deep learning in IDS not only improves the detection accuracy and efficiency of the system but also expands its ability to deal with complex network environments and new threats. With the advancement of technology and the continuous expansion of application scenarios, deep learning technology will continue to play an essential role in the field of network security, providing strong support for the protection of network resources and data security.

3. Methodology

In recent years, deep learning has achieved good results in the fields of speech recognition, image recognition, and natural language processing. Deep learning can extract abstract high-level features from original features without the need for feature selection based on expert experience. Due to its strong learning ability, scholars at home and abroad have tried to apply deep learning technology to the field of network security. Although the above method has achieved good results, it only uses the official training set in model training and testing, which has certain limitations. In addition, there are 17 more attack methods in the official test set than in the official training set. Therefore, this paper adopts the official training set and the official test set, respectively, in the training and testing of the model, which is conducive to improving the robustness of the model.

In this paper, a convolutional neural network-based intrusion detection model (CNN-Focal) is proposed. In this model, threshold convolution and Soft-max in Convolutional Neural Network (CNN) are applied to the field of intrusion detection for multi-classification, and the Focal Loss function is used to optimize unbalanced data sets, effectively improving the accuracy of intrusion detection.

3.1. CNN-Focal Intrusion Detection Model

1. Basic principles of convolutional neural networks

In the field of deep learning, a Convolutional Neural Network (CNN) is an efficient neural network model that has become a research hotspot in many fields. The basic structure of the convolutional neural network consists of the input layer, convolutional layer, pooling layer, fully connected layer, and output layer, as shown in Figure 2. In a model, there can be one or more convolution layers, pooling layers, and fully connected layers, in which the convolution layer and pooling layer generally appear alternately, that is, the convolution layer connects the pooling layer, or the convolution layer connects the pooling layer after the pooling layer, and so on. The fully connected layer generally follows the pooled layer.

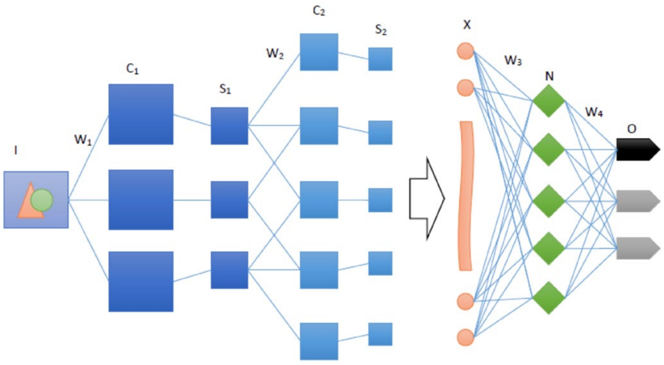

Figure 2. CNN model architecture diagram.

Each neuron in the fully connected layer is fully connected with all the neurons in the previous layer and is located at the end of the CNN structure. Usually, after the whole connection layer, the output layer is the classification layer. The output layer classifies the features extracted by the convolutional neural network, and the output of the classification is the result.

Softmax regression is a generalization of the Logistic regression model and is mainly used for multiple classifications. Softmax regression degenerates into Logistic regression when two classifications are performed. In the multi-classification problem, the class label y takes more than two values; that is, the class label y has k(an integer greater than 2) different values. Given data set {(x1, y1), (x2, y2),... , (xn, yn)}, yi denotes the class i label, i ∈ {1,2,... k}. For a given x, Softmax regression estimates the probability of x in each class of class k labels.

Loss function (Loss function) is used to evaluate the difference between the predicted value f(x) and the actual value Y of the model, usually expressed as L(Y, f(x)). The loss function reflects the

doi:10.20944/preprints202407.0595.v1

robustness of the model; that is, the smaller the loss function value, the better the robustness of the model.

2. Network structure

Intrusion detection is a classification problem that can be trained by supervised learning and then used to predict unknown data. When using convolutional neural networks, the input data of the input layer is usually two-dimensional, and the intrusion record is one-dimensional data. Therefore, in terms of convolutional operation selection, this paper adopts the one-dimensional convolution method to carry out the convolution operation on the intrusion record data. According to the NSL-KDD label imbalance and the actual classification performance of the model, the CNN-Focal model was designed in this paper, and its structure is shown in Figure 3. The CNN-Focal model has ten layers, including one input layer, three convolutional layers, 3 Dropout layers, 1 Max-pooling layer, one complete connection layer, and 1 Softmax layer.

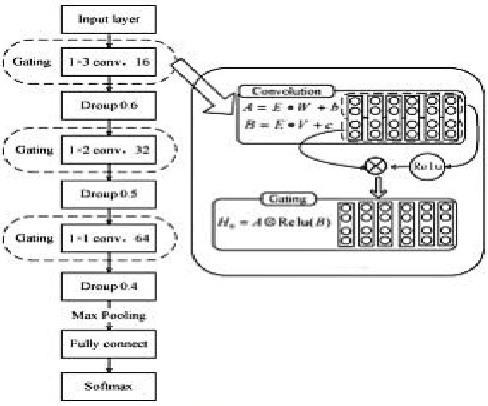

Figure 3. The CNN-Focal model.

3. The model is described as follows:

1) Input layer: The first layer is the input layer. Intrusion records are one-dimensional data. After data standardization and one hot preprocessing, the data of a single intrusion record is converted from 1 × 41 to 1 × 122.

2) Convolution layer: Layers 2, 4, and 6 are convolution layers. The concept of threshold convolution is used in the convolution layer, which is divided into two parts: one is the activation value of the convolution, namely B; The other part is directly linear, and you get the convolution, which is A. The two parts, A and B, are multiplied together to get the corresponding convolution value. Many literatures have proved that smaller convolutional nuclear energy can obtain better local features and classification performance. Therefore, CNN-Focal adopts a small convolutional kernel strategy for the design of the size of convolutional nuclei. The size of convolutional nuclei is 1 × 3, 1 × 2, and 1 × 1, and the number of convolutional nuclei is 16, 32, and 64, respectively. In addition, the small convolution kernel can cluster the learned features, alleviating the influence of convolution redundancy on model performance to a certain extent.

3) Dropout layer: The convolutional neural network model is prone to overfitting during training, which significantly affects the actual performance of the model. To mitigate this problem, Layers 3, 5, and 7 of the CNN-Focal models employ Dropout. The sizes of Dropout values are set to 0.6, 0.5, and 0.4, respectively, based on the actual classification effect of the CNN-Focal model.

4) Max-Pooling layer: The pooling layer can reduce the calculation amount. The 8th layer of the CNN-Focal model is the Max-Pooling layer, with a stride of 2; that is, the number of parameters is reduced to half of the original.

5) Fully connected layer: The number of fully connected layer neurons in CNN-Focal is 200.

6) SoftMax layer: In deep learning, SoftMax regression is often used as a standard classifier for multi-classification or binary classification problems. CNN-Focal uses SoftMax regression as a multi-classifier.

3.2. Experimental Design

In this paper, the Focal Loss function is applied to the model. To verify the effectiveness of Focal Loss, this paper conducted an experimental comparison between Focal Loss and the cross-entropy loss function commonly used in deep learning; that is, the loss function of the CNN-Focal model was replaced with a cross-entropy loss function, and the model with the changed loss function was recorded as CNN-Cross. In addition, to the better classification effect of the CNN-Focal model, this paper compares CNN-Focal with SVM, Random Forest, Decision Tree, and GaussianNB.

In the field of intrusion detection, NSL-KDD data sets are widely used. In this paper, the data preprocessed NSL-KDD data sets are used for CNN-Focal and comparison model training and testing. In addition, this paper selected precision, accuracy, recall rate, F1 score, and other indicators to evaluate the model.

1) Data set introduction. In the research of intrusion detection, the KDD CUP 99 dataset is the most widely used dataset. There are about 5 million records in the training set and about 300,000 records in the test set in the KDD CUP 99 data set. The amount of data in this data set has high requirements on the experimental hardware environment. In addition, various statistical analyses show that there are a large number of redundant records in the KDD CUP 99 dataset, which will cause the model to overfit and require more computer resources in the training process, and the model convergence is slow.

Table 1. Data set.

Dataset Name	Training Set Size	Test Set Size	Number of Features	Label Categories
NSL-KDD	125973	22543	41	Normal, Probe, Dos, U2L, R2L
NSL-KDD	125973 instances	22543 instances	41	Normal, Probe, R2L, U2R, DoS
NSL-KDD	Large	Small	41	Normal, Probe, Dos, R2L, U2R
NSL-KDD	125973 records	22543 records	41	Normal, Probe, DoS, U2R, R2L
NSL-KDD	Comprehensive	Limited	41	Normal, Probe, Dos, U2L, R2L

The NSL-KDD dataset solves the problems existing in the KDD CUP 99 dataset, and many research results are based on the NSL-KDD dataset. The NSL-KDD dataset contains 41 columns of features and 1 column of labels. The label columns are divided into five categories: Normal, Probe, Dos, U2L, and R2L. The order of magnitude of this data set does not require high requirements for the experimental hardware environment, and experiments can be carried out on ordinary machines. In addition, the training set and the test set contain different attack methods, so the model trained using this data set has a better detection effect for new attacks.

3.3. Data Preprocessing

Two data types, nominal and numerical, are generally used. The 41 columns of feature attribute values in the NSL-KDD dataset have both nominal and numerical values. The attribute value types of protocol_ type, service, flag, and label in the data set are nominal, and the rest are numerical. Normalization of data is the scaling of data to a specific interval so that it falls from a large interval into a cell. The standardized data can shorten the convergence time of the model and improve its accuracy. In this paper, the numerical features are standardized and scaled to between [0,1]. One-hot coding, also known as single-heat coding, can not only deal with the features of non-continuous numerical values but also make the distance between the features more reasonable. In this paper, the OneHotEncoder in the scleral package is used to one-hot encode the protocol_ type, service, flag and label four columns of nominal data.

Evaluation index. To evaluate the model, we need not only a practical and feasible experimental scheme but also an evaluation index to measure the generalization ability of the model, which is the performance measurement. In the unbalanced classification task, the most commonly used performance measures are Accuracy, Precision, Recall, and F1 score.

3.4. Experimental Resul

Model	Dataset Used	Training Method	Evaluation Metrics	Results Summary
CNN-Focal	NSL-KDD	Train-test split (70%-30%)	Accuracy, Precision, Recall, F1-score	Achieved high accuracy and balanced performance across all metrics. The model effectively addressed class imbalance using Focal Loss.
CNN-Cross	NSL-KDD	Train-test split (70%-30%)	Accuracy, Precision, Recall, F1-score	Compared performance with CNN-Focal using Cross Entropy Loss, showing differences in effectiveness in handling class imbalance.
SVM	NSL-KDD	Train-test split (70%-30%)	Accuracy, Precision, Recall, F1-score	Provided benchmark for traditional machine learning approach in intrusion detection, showing competitive results.
RandomForest	NSL-KDD	Train-test split (70%-30%)	Accuracy, Precision, Recall, F1-score	Demonstrated ensemble learning's effectiveness in handling complex feature relationships.
DecisionTree	NSL-KDD	Train-test split (70%-30%)	Accuracy, Precision, Recall, F1-score	Showed basic decision-making capability with moderate performance metrics.

The experiments on the NSL-KDD dataset highlighted the effectiveness of the CNN-Focal model in improving intrusion detection accuracy through advanced deep learning techniques. Here are the key conclusions:

1. Model Performance: CNN-Focal outperformed traditional methods like SVM, Random Forest, and Decision Tree in terms of accuracy, precision, recall, and F1-score. It showcased robustness in handling the dataset's class imbalance using Focal Loss.
2. Comparison with CNN-Cross: Comparing CNN-Focal with CNN-Cross (using Cross Entropy Loss) showed that Focal Loss significantly enhanced the model's ability to classify minority classes, which is crucial for real-world intrusion detection scenarios.
3. Dataset Suitability: NSL-KDD dataset's partition into training and testing sets facilitated robust evaluation of model performance across different attack types, enhancing model generalization.
4. Future Directions: Future research could explore hybrid models combining CNN architectures with traditional machine learning algorithms for enhanced accuracy and efficiency in intrusion detection.

This conclusion synthesizes the experimental findings, emphasizing CNN-Foal's suitability and superiority in handling intrusion detection tasks compared to traditional methods.

4. Conclusion

With the rapid development of information technology, the issue of network security has increasingly become a focal point of global attention. This paper examines the current landscape and challenges of network security, explores the application of deep learning and artificial intelligence in defense strategies, and proposes future-oriented approaches. The continual evolution of cyber threats presents new challenges to traditional cybersecurity defenses. Signature-based methods are inadequate against novel and unidentified network attacks, necessitating the development of advanced defense technologies. Deep learning, as an advanced machine learning technology, has made significant strides in fields like image recognition and natural language processing. Its application in network security enhances detection and defense capabilities against threats such as malware and phishing attacks.

Furthermore, artificial intelligence offers automated network security defense capabilities, enabling real-time monitoring, analysis of network traffic, and prompt responses to security incidents. AI also aids security experts in gathering and analyzing threat intelligence, thereby improving the efficiency and accuracy of network security defense. This paper proposes an integrated model of deep learning and artificial intelligence for network security defense, forecasting future trends in defense strategies. Future network security defenses will be more intelligent, automated, and adaptable to evolving network environments. As technology continues to advance, new defense technologies will emerge, bolstering network security.

In conclusion, deep learning and artificial intelligence hold immense potential for enhancing network security defenses. Continued optimization and advancement of these technologies will help establish a more secure and reliable digital environment, supporting the growth of the digital economy. Addressing cyber security challenges requires collaborative efforts from governments, enterprises, academia, and other stakeholders to safeguard cyberspace's security and stability."

This revision improves grammar, coherence, and logical flow while maintaining the original content's meaning and emphasis on the application of deep learning and artificial intelligence in network security.

References

1. Sagduyu, Yalin E., Yi Shi, and Tugba Erpek. "IoT network security from the perspective of adversarial deep learning." 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2019.
2. Alom, M. Z., & Taha, T. M. (2017, June). Network intrusion detection for cyber security using unsupervised deep learning approaches. In 2017 IEEE National Aerospace and Electronics Conference (NAECON) (pp. 63-69). IEEE.
3. Kumar, C., Bharati, T. S., & Prakash, S. (2021). Online social network security: a comparative review using machine learning and deep learning. Neural Processing Letters, 53(1), 843-861.
4. Gong Y, Zhu M, Huo S, et al. Utilizing Deep Learning for Enhancing Network Resilience in Finance[C]//2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2024: 987-991.
5. Uppal, H. A. M., Javed, M., & Arshad, M. (2014). An overview of the intrusion detection system (IDS) along with its commonly used techniques and classifications. *International Journal of Computer Science and Telecommunications*, *5*(2), 20-24.
6. Abbas, S. H., Naser, W. A. K., & Kadhim, A. A. (2023). Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Global Journal of Engineering and Technology Advances*, *14*(2), 155-158.
7. Pradhan, M., Nayak, C. K., & Pradhan, S. K. (2020). Intrusion detection systems (IDS) and their types. In *Securing the Internet of things: Concepts, methodologies, tools, and applications* (pp. 481-497). IGI Global.
8. Tian, J., Li, H., Qi, Y., Wang, X., & Feng, Y. (2024). Intelligent medical detection and diagnosis assisted by deep learning. Applied and Computational Engineering, 64, 121-126.
9. Borkar, A., Donode, A., & Kumari, A. (2017, November). A survey on the Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS). In *2017 International Conference on Inventive Computing and Informatics (ICICI)* (pp. 949-953). IEEE.
10. Liu, B., Cai, G., Ling, Z., Qian, J., & Zhang, Q. (2024). Precise positioning and prediction system for autonomous driving based on generative artificial intelligence. Applied and Computational Engineering, 64, 42-49.

11. Wang, B., He, Y., Shui, Z., Xin, Q., & Lei, H. (2024). Predictive optimization of DDoS attack mitigation in distributed systems using machine learning. Applied and Computational Engineering, 64, 95-100.
12. Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, *2*(1), 1-4.
13. Cui, Z., Lin, L., Zong, Y., Chen, Y., & Wang, S. (2024). Precision gene editing using deep learning: A case study of the CRISPR-Cas9 editor. Applied and Computational Engineering, 64, 134-1
14. Xiao, J., Wang, J., Bao, W., Deng, T. and Bi, S., Application progress of natural language processing technology in financial research.
15. Choudhury, M., Li, G., Li, J., Zhao, K., Dong, M., & Harfoush, K. (2021, September). Power Efficiency in Communication Networks with Power-Proportional Devices. In *2021 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-6). IEEE.
16. Yuan, J., Lin, Y., Shi, Y., Yang, T., & Li, A. (2024). Applications of Artificial Intelligence Generative Adversarial Techniques in the Financial Sector. Academic Journal of Sociology and Management, 2(3), 59-66.
17. Haowei, Ma, et al. "CRISPR/Cas-based nanobiosensors: A reinforced approach for specific and sensitive recognition of mycotoxins." Food Bioscience 56 (2023): 103110.
18. Yu, D., Xie, Y., An, W., Li, Z., & Yao, Y. (2023, December). Joint Coordinate Regression and Association For Multi-Person Pose Estimation, A Pure Neural Network Approach. In *Proceedings of the 5th ACM International Conference on Multimedia in Asia* (pp. 1-8).
19. Kumar, S., Gupta, S., & Arora, S. (2021). Research trends in network-based intrusion detection systems: A review. *Ieee Access*, *9*, 157761-157779.
20. Lin, Y., Li, A., Li, H., Shi, Y., & Zhan, X. (2024). GPU-Optimized Image Processing and Generation Based on Deep Learning and Computer Vision. Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023, 5(1), 39-49.
21. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.
22. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50.
23. Sekar, R., Guang, Y., Verma, S., & Shanbhag, T. (1999, November). A high-performance network intrusion detection system. In *Proceedings of the 6th ACM Conference on Computer and Communications Security* (pp. 8-17).
24. Huang, C., Bandyopadhyay, A., Fan, W., Miller, A., & Gilbertson-White, S. (2023). Mental toll on working women during the COVID-19 pandemic: An exploratory study using Reddit data. PloS one, 18(1), e0280049.
25. Ma, Haowei. "Research on promotion of lower limb movement function recovery after stroke by using lower limb rehabilitation robot in combination with constant velocity muscle strength training." *2021 7th international symposium on mechatronics and industrial informatics (ISMII)*. IEEE, 2021.
26. Bi, Shuochen, Wenqing Bao, Jue Xiao, Jiangshan Wang, and Tingting Deng. "Application and practice of AI technology in quantitative investment." *arXiv preprint arXiv:2404.18184*(2024).
27. Liang, P.; Song, B.; Zhan, X.; Chen, Z.; Yuan, J. Automating the training and deployment of models in MLOps by integrating systems with machine learning. Appl. Comput. Eng. 2024, 67, 1–7, https://doi.org/10.54254/2755-2721/67/20240690.
28. Haowei, M. A., et al. "Employing Sisko non-Newtonian model to investigate the thermal behavior of blood flow in a stenosis artery: Effects of heat flux, different severities of stenosis, and different radii of the artery." *Alexandria Engineering Journal* 68 (2023): 291-300.
29. Li, A., Yang, T., Zhan, X., Shi, Y., & Li, H. (2024). Utilizing Data Science and AI for Customer Churn Prediction in Marketing. *Journal of Theory and Practice of Engineering Science*, *4*(05), 72-79.
30. Farnaaz, N., & Jabbar, M. A. (2016). Random forest modeling for network intrusion detection system. *Procedia Computer Science*, *89*, 213-217.
31. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.
32. Zhang, Y.; Liu, B.; Gong, Y.; Huang, J.; Xu, J.; Wan, W. Application of machine learning optimization in cloud computing resource scheduling and management. Appl. Comput. Eng. 2024, 64, 17–22, https://doi.org/10.54254/2755-2721/64/20241359.
33. Huang, J.; Zhang, Y.; Xu, J.; Wu, B.; Liu, B.; Gong, Y. Implementation of seamless assistance with Google Assistant leveraging cloud computing. Appl. Comput. Eng. 2024, 64, 170–176, https://doi.org/10.54254/2755-2721/64/20241383.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.