Mathematical Modeling and Algorithm Application
ISSN: 3006-0842 | Vol. 6, No. 3, 2025

Research on Cybersecurity Evaluation Algorithms for Computer Networks Based on Deep Learning

Meiyu Shen*

School of Big Data, Baoshan University, Baoshan 678000, China
* **Corresponding author**: Meiyu Shen (Email: 2051255603@qq.com)

Abstract: With the deepening development of the digital age, computer networks have become the core infrastructure for information exchange in modern society. However, they also face numerous security threats, such as data leaks and cyberattacks. Traditional network security protection measures are ineffective against complex attacks, and more intelligent solutions are urgently needed. Deep learning technology, with its superior feature learning capabilities, can automatically identify abnormal patterns in network traffic, improving the detection and defense capabilities against network threats. This paper focuses on the application of deep learning in computer network security assessment and constructs a deep learning network security assessment algorithm. Through a process consisting of data collection and processing, feature extraction, and model training, this algorithm accurately identifies network attack behaviors under real-time monitoring. Experimental results show that compared with traditional methods, the deep learning-based security assessment algorithm achieves significant improvements in accuracy, recall, and F1 score, demonstrating strong application value and promising prospects. By learning from historical data, the algorithm also provides proactive defense strategies for network security, providing technical support for protecting network security.

Keywords: Deep Learning; Computer Network Security; Network Security Evaluation Algorithm; Intrusion Detection; Malicious Code Identification

1. Introduction

1.1. Research Background and Significance

With the deepening development of the digital age, computer networks have become the core infrastructure for information exchange and data transmission in modern society. The rapid evolution of network technology has brought unprecedented convenience to human life and promoted the digital transformation of the global economy. Security threats such as data leakage, network attacks, and malware transmission pose a serious threat to personal privacy, corporate secrets, and even national security [1] . Cybersecurity incidents such as hacker attacks, network viruses, and data leaks occur frequently, causing huge losses to individuals, businesses, and society [2] .

Traditional network security protection technologies are unable to cope with increasingly complex and diverse attack methods, and more intelligent and efficient security protection solutions are urgently needed. Deep learning algorithms, as an important branch of artificial intelligence, have achieved remarkable results in various fields such as computer vision and natural language processing due to their powerful feature learning and representation capabilities. Deep learning technology can automatically learn the inherent patterns and patterns of network traffic, enabling more accurate detection and defense against various network attacks.

Deep learning is widely used in the field of network security, including intrusion detection, vulnerability discovery, and malicious code detection. Research on deep learning-based computer network security evaluation algorithms has important theoretical and practical significance. From a theoretical perspective, this research will promote the in-depth application of deep learning theory in network security and enrich the technical framework for network security protection. From a practical perspective, the design of appropriate deep learning models and structures can significantly improve the accuracy and efficiency of network security identification, providing technical support for building a more secure and reliable network environment.

1.2. Research Objectives and Problem Definition

The core objective of this study is to construct a computer network security evaluation algorithm system based on deep learning technology. By designing a reasonable deep learning model and structure, the accuracy and efficiency of network security identification can be improved. The research aims to solve the problems of insufficient accuracy and poor real-time performance of traditional network security evaluation methods in the face of complex and changing network threats, and establish an intelligent evaluation mechanism that can automatically learn the inherent laws and patterns of network traffic.

Traditional network security defense methods can no longer meet the needs of combating new threats [3-4] . The key issues facing the current network security field include: how to effectively identify and classify various types of network security threats, how to improve the detection ability of unknown attacks, and how to establish an accurate network security situation assessment mechanism. Deep learning algorithms, with their powerful feature learning and representation capabilities, can extract and abstract high-level feature representations layer by layer from raw input data by constructing neural network models with multi-layer nonlinear transformations.

In terms of problem definition, this study focuses on three core issues: firstly, how to design a deep learning model architecture suitable for network security evaluation, so that it can effectively handle the complexity and diversity of network traffic data; Secondly, how to construct a

comprehensive network security evaluation index system to achieve unified evaluation of multiple dimensions such as intrusion detection, security vulnerability mining, and malicious code detection; The third is how to optimize algorithm performance while ensuring evaluation accuracy and meeting the needs of real-time monitoring of network security. By addressing these issues, this study aims to provide a more intelligent and efficient evaluation method for the field of network security.

2. Literature Review

2.1. Current Status of Computer Network Security

In the context of the digital age, computer network security is facing unprecedented challenges. The methods of cyber attacks are becoming increasingly complex and diverse, ranging from traditional virus transmission to modern advanced persistent threats, and security threats are showing a diversified development trend [5] . Malicious software spreads rapidly through various channels such as email, file downloads, instant messaging, etc., not only disrupting the normal operation of computer systems, but also potentially stealing sensitive user information, leading to the paralysis of the entire network infrastructure [6] . As an important threat source to network security, hacker attacks include system intrusion, phishing websites, data tampering, etc. These attack behaviors bring huge economic losses and information security risks to enterprises and individuals [7].

Network security threats not only come from external attacks, but also from internal threats that cannot be ignored. Internal personnel within the organization may pose security risks due to negligence, malicious behavior, or improper operations, including sensitive information leakage, system damage, and other issues [8] . External threats mainly manifest in the form of information interception, illegal access, and data integrity destruction. Attackers use various technical means to break through the network protection system and obtain unauthorized access permissions. Frequent security incidents such as data breaches and privacy violations not only threaten users' personal information security, but also have profound impacts on social stability and national security [9] .

The current network security assessment technology faces many challenges, lacking unified assessment standards and a recognized risk level classification system [10] . The traditional evaluation methods have the problem of insufficient universality in dealing with the evaluation of enterprise network security operation capabilities, especially when facing complex data with multi-dimensional indicators. The existing methods are difficult to meet practical needs [11] . With the continuous emergence of new types of network attack methods, network security risk assessment technology needs to continue to develop and improve to cope with the increasingly complex security threat environment.

2.2. Application of Deep Learning in Network Security

As an important branch of artificial intelligence, deep learning algorithms have shown great potential in the field of computer network security due to their powerful feature learning and representation capabilities. Through multi-layer nonlinear transformation neural network models, deep learning can extract and abstract high-level feature representations layer by layer from raw network data, achieving accurate recognition and efficient processing of complex network attack behaviors.

The application of deep learning in network security has covered multiple key areas. In intrusion detection systems (IDS), deep learning algorithms can automatically identify abnormal patterns and detect potential attacks by analyzing network traffic and user behavior data [12] . In the area of malicious code detection, deep learning technology can deeply analyze large-scale malicious code samples and learn the inherent characteristic patterns of malware, thereby effectively identifying unknown malicious code [13-14] . The field of security vulnerability discovery also benefits from the powerful analytical capabilities of deep learning, automatically discovering potential security weaknesses in the system.

The development of proactive defense strategies for network security benefits from the intelligent nature of deep learning. This strategy can automatically learn the characteristics and patterns of network security threats, monitor network traffic in real-time, and detect and prevent attack behaviors in a timely manner. The application of deep learning in network security defense systems has endowed the system with stronger intelligence and adaptability, enabling it to cope with increasingly complex network security threat environments.

3. Research Methods

3.1. Data Collection and Processing

The effectiveness of computer network security evaluation algorithms depends largely on the comprehensiveness of data collection and the accuracy of data processing. Network security data is multi-source and heterogeneous, encompassing network device logs, host audit logs, security device alarm information, business system operation logs, and other types. These data sources have diverse formats and varying data quality, necessitating the establishment of a comprehensive data collection and preprocessing system.

The data collection phase requires the construction of a distributed data collection framework to capture network traffic characteristics and security event information in real time. The main challenges faced during the collection process include data storage, data cleaning, data mining, data analysis, and data security. To address these technical challenges, the system utilizes advanced distributed storage systems, efficient data processing algorithms, and strict data security measures.

Table 1 Data Collection and Processing Methods

Data Type	Collection Frequency	Data volume (GB-day)	Processing Method
Network Traffic Log	Real-Time	50-100	Streaming
Security Device Alarm	Real-Time	10-20	Batch Processing
Host Audit Log	Hourly	20-40	Periodic Processing
Business System Log	Minutely	30-60	Hybrid Processing

Data preprocessing includes three core steps: data integration, data cleaning, and feature extraction. Data integration unifies heterogeneous data from various sources into a standardized format and establishes a unified data model. Data cleaning improves data quality through outlier detection and missing value imputation techniques. Feature extraction leverages the automated feature learning capabilities of deep learning to extract high-level, abstract feature representations from the raw data.

$$F_{processed} = \phi(\theta, X_{raw}) \quad (1)$$

Where $F_{processed}$ represents the processed feature vector, ϕ is the feature extraction function, θ is the deep learning model parameter, and X_{raw} is the original input data. Through this mathematical model, the system can automatically learn the inherent laws and patterns of network traffic, providing high-quality input features for subsequent security assessments.

3.2. Deep Learning Model Construction

The construction of a deep learning model is the core step in implementing network security assessment algorithms. Leveraging the nonlinear transformation capabilities of multi-layer neural networks, the system can automatically extract high-level security feature representations from raw network data. The model construction process must consider the complexity and diversity of network security data and design an appropriate network architecture to handle different types of security threat patterns.

Convolutional neural networks (CNNs), as the primary component for feature extraction, can effectively identify local patterns and abnormal behavior characteristics in network traffic. The model utilizes a multi-layer convolutional architecture. Through deep learning operations in convolutional and pooling layers, the system intelligently extracts key features of network data, enabling efficient detection of unknown attacks. The introduction of long short-term memory (LSTM) layers addresses the temporal dependency of sequential data and can capture the temporal characteristics of network attack behavior. The fully connected layer serves as a classifier to output the final security assessment result, using the softmax activation function to predict the probability distribution of multi-category threats.

Model training uses the backpropagation algorithm for parameter optimization. The loss function is designed to combine cross-entropy loss with a regularization term. The mathematical expression is:

$$L = -\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{C} y_{ij}\log(\hat{y}_{ij}) + \lambda \quad (2)$$

Where N is the number of samples and C is the number of categories. y_{ij} is the true label, $\hat{y}_{ij}$ is the predicted probability, and λ is the regularization coefficient. Through iterative learning of a large amount of training data, the model continuously adjusts network parameters to minimize prediction errors, thereby improving generalization ability and performance.

4. Algorithm Design and Implementation

4.1. Evaluation Algorithm Design

4.1.1. Algorithm Flowchart

The design of the deep learning-based computer network security evaluation algorithm adopts a multi-layered processing architecture, building a scientific and rational algorithmic process to achieve intelligent identification and assessment of network security threats. The algorithmic process begins with data preprocessing and progresses through feature extraction, model training, and security evaluation. Each step fully leverages the advantages of deep learning technology to enhance network security protection capabilities.

The core processing flow of the algorithm consists of four main stages: data collection and preprocessing, feature engineering, deep learning model training, and security evaluation. During the data collection stage, the system collects raw data from network traffic monitoring points, including packet header information, traffic statistics, and behavior patterns. The preprocessing module cleans, normalizes, and converts the collected data to prepare for subsequent deep learning processing. The feature engineering stage utilizes an automatic feature learning mechanism to extract high-dimensional feature representations from the raw data through a multi-layer neural network.

The deep learning model training process uses a backpropagation algorithm for parameter optimization. Iterative learning on a large number of labeled samples continuously improves the model's recognition accuracy. During the security assessment phase, the trained model is applied to real-time network traffic analysis, outputting a threat level score and security status assessment results. The entire algorithm process is designed to balance real-time performance with accuracy, ensuring detection accuracy while meeting the real-time processing requirements of the network environment. Each module in the algorithm process can be independently optimized and adjusted, providing good adaptability and scalability for deployment in diverse network environments.

4.1.2. Key Technology Analysis

Computer network security assessment algorithms based on deep learning involve multiple core technologies, among which feature extraction and pattern recognition form the algorithm's fundamental architecture. Deep learning algorithms construct a neural network model with multi-layer nonlinear transformations, extracting and abstracting high-

level feature representations from the raw input data layer by layer, achieving accurate modeling and efficient processing of complex data. The algorithm utilizes optimization techniques such as the backpropagation algorithm, iteratively learning from a large amount of training data, continuously adjusting network parameters to minimize prediction error, thereby improving the model's generalization and performance.

Network traffic analysis and threat identification technology are important tools for security assessment. Deep learning technology can automatically learn the inherent patterns and patterns of network traffic, enabling more accurate detection and defense against various network attacks. The algorithm can deeply analyze large-scale network traffic and malicious code to automatically learn and identify potential security threat patterns, thereby enabling real-time detection of unknown attacks. This technology has wide applications in intrusion detection, security vulnerability discovery, and malicious code detection.

Security situation assessment and risk quantification mechanisms are core components of algorithm design. Leveraging the powerful pattern recognition and learning capabilities of deep learning, cybersecurity professionals can more intelligently respond to complex and ever-changing network threats. The evaluation algorithm utilizes a multi-dimensional indicator system, combining real-time monitoring data with historical threat patterns to construct a security risk assessment model. This model utilizes the principle of loss function optimization to improve evaluation accuracy by minimizing prediction error:

$$L = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 + \lambda \sum_{j=1}^{m} w_j^2 \quad (3)$$

Where, L is the loss function, y_i is the actual security rating, $\hat{y}_i$ is the predicted rating, λ is the regularization parameter, and$w_j$is the network weight.

4.2. Algorithm Implementation and Optimization

4.2.1. Implementation Environment and Tools

The implementation of deep learning network security assessment algorithms requires the establishment of a comprehensive hardware and software environment support system. The experimental environment constructed in this study covers a complete technology stack, from underlying hardware to upper-level application frameworks, providing a solid foundation for efficient algorithm operation and accurate evaluation.

In terms of hardware configuration, the experimental platform utilizes a high-performance GPU cluster architecture equipped with NVIDIA Tesla V100 graphics cards, each with 32GB of video memory, capable of supporting the parallel processing of large-scale network traffic data. The CPU utilizes an Intel Xeon E5-2699 v4 processor with 22 cores, 44 threads, and a base frequency of 2.2GHz. The memory configuration is 512GB of DDR4. The storage system utilizes an NVMe SSD array with read and write speeds of up to 3.5GB/s, ensuring rapid access and processing of massive amounts of secure data. The network environment utilizes a Gigabit Ethernet connection to ensure real-time and stable transmission of training data.

For software framework selection, this study used the Paddle deep learning framework as its core development platform. Paddle integrates a core framework, tool components, and a service platform, offering outstanding distributed training capabilities in large-scale data scenarios, comprehensive algorithm encapsulation, and ease of use. The operating system used was Ubuntu 20.04 LTS, Python 3.8.10, and CUDA 11.2, along with the cuDNN 8.1.1 deep neural network library. Data processing tools included NumPy 1.21.0 and Pandas 1.3.3 for data preprocessing, and Scikit-learn 1.0.2 for machine learning algorithm support.

The development environment integrated Jupyter Notebook as an interactive development interface, facilitating algorithm debugging and result visualization. Git 2.34.1 was used for version control, and the code was hosted in a private GitLab repository to ensure traceability during the R&D process. The monitoring tool uses TensorBoard to visualize the training process, and Prometheus combined with Grafana enables real-time monitoring of system performance. The network security data collection tool integrates network analysis software such as Wireshark and tcpdump, supporting multi-protocol packet capture and analysis.

4.2.2. Optimization Strategy

Optimization strategies for deep learning models in computer network security assessment algorithms involve technical improvements at multiple levels. Improving algorithm performance requires systematic optimization of model structure, training process, and computational efficiency to meet the stringent requirements of real-time network security detection.

Model structure optimization utilizes an improved strategy for multi-layer neural network architecture. By introducing residual connections and an attention mechanism, the model can more effectively extract abnormal features from network traffic. The application of batch normalization technology helps stabilize the training process and prevent the vanishing gradient problem. Proper configuration of dropout technology effectively prevents overfitting and improves the model's generalization ability. Model compression technology significantly reduces model complexity while maintaining detection accuracy through parameter pruning and knowledge distillation.

Table 2 Application scenarios and performance improvement ratios of different optimization strategies

Optimization technology	Application scenario	Performance improvement	Computational overhead
Residual connection	Deep network training	15-20%	Low
Attention mechanism	Feature selection	10-15%	Medium
Batch normalization	Training stability	8-12%	Low
Model pruning	Inference acceleration	Maintain 95% accuracy	Significant reduction

Training strategy optimization focuses on learning rate scheduling and data augmentation techniques. The adaptive

learning rate algorithm uses an improved version of the Adam optimizer, combined with a cosine annealing strategy to dynamically adjust the learning step size. Data augmentation enhances the model's ability to recognize complex attack patterns through adversarial sample generation and noise injection techniques.

Computational efficiency optimization strategies include the application of parallel computing and caching mechanisms. GPU parallel training significantly reduces training time by combining data parallelism and model parallelism. The feature cache mechanism precomputes and stores frequently accessed network traffic features, reducing repetitive computing overhead. The pipeline processing architecture parallelizes data preprocessing, feature extraction, and classification decisions to achieve real-time detection performance requirements.

5. Experiments and Results Analysis

5.1. Experimental Design and Implementation

5.1.1. Experimental Dataset Selection

The selection of experimental dataset has a decisive influence on the performance of deep learning models in network security evaluation. This study carefully selected representative standard datasets from three dimensions: network traffic analysis, malicious code detection, and intrusion behavior identification, to ensure the reliability and validity of the algorithm evaluation results. Deep learning applications in the field of network security require large-scale, high-quality training data to build accurate threat identification models.

For the network traffic anomaly detection task, the NSL-KDD dataset was selected as the primary evaluation benchmark. This dataset contains 156,098 normal network connection records and 25,192 attack samples, covering four major categories: DoS attacks, probing attacks, privilege escalation attacks, and remote access attacks. The CICIDS-2017 dataset was also used for supplementary validation. This dataset provides more realistic network environment simulation data and contains 2,830,743 records, of which approximately 12% are malicious traffic. To verify the algorithm's malware detection capabilities, 10,000 malicious file samples from the VirusShare malicious sample library and 100,000 benign file samples from the EMBER dataset were used.

During the data preprocessing phase, standardization and feature engineering techniques were used to clean and transform the raw data. Data augmentation techniques were used to expand the training set to 1.5 times its original size, and the training, validation, and test sets were divided in a ratio of 7:2:1. Deep learning algorithms can automatically learn and identify potential security threat patterns by deeply analyzing large-scale network traffic and malicious code.

Table 3 Experimental Dataset Selection

Dataset Type	Dataset Name	Total Number of Samples	Malicious Sample Ratio	Feature Dimension
Network Traffic	NSL-KDD	181,290	13.9%	41
Network Traffic	CICIDS-2017	2,830,743	12.0%	78
Malware	VirusShare	10,000	100%	2,381
Benign Files	EMBER	100,000	0%	2,381

5.1.2. Experimental Procedures and Methods

This study employed a systematic experimental design to validate the effectiveness of a deep learning-based network security assessment algorithm. The experimental process included key steps such as data preprocessing, model training, and testing and validation, as detailed in the table below. A rigorous methodology ensured the reliability and accuracy of the experimental results.

Table 4 Description of experimental stages and methods

Experimental stage	Method description	Evaluation indicators	Data ratio
Data preprocessing	Standardization, feature extraction	Data quality score	100%
Model training	Deep neural network training	Training loss, validation accuracy	70%
Model validation	Cross-validation	Precision, recall	20%
Performance test	Independent test set evaluation	F1 score, AUC value	10%

The experiment used stratified sampling to extract training samples from the selected dataset, splitting the data into training, validation, and test sets in a 70%:20%:10% ratio. During data preprocessing, standardization techniques were used to convert network traffic feature data into a format suitable for deep learning model input. Corresponding feature vectors were established for different types of network security threats to ensure the model effectively learns the inherent patterns of various attack patterns. Parameter optimization was performed using the backpropagation algorithm, employing the Adam optimizer with a learning rate decay strategy to ensure stable and efficient model convergence.

Model performance was evaluated using a multi-dimensional metric system, including classic evaluation metrics such as accuracy, precision, recall, and F1 score. A comparative experiment was designed to compare the proposed deep learning evaluation algorithm with traditional machine learning methods. The k-fold cross-validation method was used during testing to reduce the impact of

random error on the results through multiple repetitions. Detailed performance metrics and runtime were recorded for each experimental run to provide sufficient data support for subsequent analysis.

The model loss function used in the experiment adopts cross-entropy loss, and its mathematical expression is:

$$Loss = -\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{C} y_{ij}\log(p_{ij}) \quad (4)$$

Where N represents the number of samples and C represents the number of categories.$y_{ij}$is the true label,p_{ij}To predict probability.

5.2. Result Analysis and Discussion

5.2.1. Evaluation of Experimental Results

The deep learning based network security evaluation algorithm constructed in this study exhibits excellent performance in multiple dimensions. Deep learning algorithms extract and abstract high-level feature representations layer by layer from raw input data by constructing neural network models with multiple layers of nonlinear transformations, achieving accurate modeling of complex network security data. The experiment uses a standard network security dataset for training and testing, covering multiple application scenarios such as intrusion detection, malicious code recognition, and abnormal behavior monitoring.

Table 5 Comparison of Experimental Results

Evaluation indicators	traditional method	This algorithm	increase margin
Accuracy (%)	82.3	94.7	15.1%
Recall rate (%)	78.9	91.2	15.6%
F1 score (%)	80.5	92.9	15.4%
False alarm rate (%)	8.2	3.1	-62.2%
Detection time (ms)	45.6	28.3	-38.0%

Experimental results show that this algorithm achieves significant improvements in key metrics such as precision, recall, and F1 score. Compared with traditional machine learning methods, deep learning algorithms demonstrate significant advantages in network intrusion detection due to their strong ability to express deep features and excellent classification results. They also possess strong generalization capabilities for detecting unknown attack patterns and can automatically learn the inherent laws and patterns of network traffic, thereby more accurately detecting and defending against various network attacks.

By learning from a large amount of network traffic and attack behavior, deep learning algorithms can identify and understand complex attack patterns, improving the accuracy and timeliness of attack detection. Experimental results have shown that active defense strategies for network security based on deep learning can effectively improve the level of network security and reduce network security risks. Algorithms demonstrate good real-time performance and stability in processing massive network data, laying a solid foundation for practical applications.

5.2.2. Practical Significance of the Results

Computer network security evaluation algorithms based on deep learning have demonstrated significant value and broad application prospects in practical applications. This algorithm, through in-depth analysis of large-scale network traffic and malicious code, automatically learns and identifies potential security threat patterns, enabling real-time detection of unknown attacks. This automated threat identification capability provides powerful technical support for network administrators, enabling them to promptly identify and respond to various complex network security threats.

The application of deep learning technology in network security has significantly enhanced protection capabilities in areas such as intrusion detection, malicious code identification, and abnormal behavior monitoring. The algorithm automatically extracts high-level features to accurately identify and classify security vulnerabilities, making it more effective than traditional methods. This intelligent security protection mechanism not only improves detection accuracy but also significantly reduces false alarm rates and reduces the need for manual intervention.

The practical significance of this algorithm is also reflected in its significant improvement in network security prediction and analysis capabilities. Through deep learning of historical data, the system is able to identify potential attack patterns and deploy proactive defense strategies. This predictive protection mechanism shifts network security from passive response to active prevention, providing an advanced means of protection for the network security of critical infrastructure. In practical deployment, this algorithm can help network administrators discover network security issues in a timely manner and take effective measures to ensure the safe and stable operation of the network.

6. Conclusion and Prospect

This study explores the application of deep learning technology in the field of computer network security evaluation and successfully constructs a network security evaluation algorithm system based on deep learning. Research has shown that deep learning algorithms can extract and abstract high-level feature representations layer by layer from raw network traffic data by constructing neural network models with multi-layer nonlinear transformations, achieving accurate identification and efficient processing of complex network security threats. The experimental results demonstrate that the proposed evaluation algorithm has significantly improved the accuracy and efficiency of network security threat detection.

Deep learning technology has demonstrated powerful feature learning and representation capabilities in the field of network security, which can automatically learn the inherent laws and patterns of network traffic, thereby more accurately detecting and defending against various network attack

behaviors. The evaluation algorithm designed by this research institute can not only automatically identify and classify network security threats, but also monitor network traffic in real time, detect and warn potential security risks in a timely manner. This proactive defense strategy effectively enhances network security protection capabilities and provides a new technological path for dealing with increasingly complex network security environments.

With the continuous development of network technology, security issues such as data leakage, network attacks, and malware propagation pose an increasingly serious threat to personal privacy, corporate secrets, and even national security. Future research should focus on optimizing the real-time performance of algorithms and improving the generalization capabilities of models, exploring more intelligent network security defense mechanisms. At the same time, it is necessary to further improve the adaptive capabilities of deep learning models in the face of new network attacks, build a more comprehensive and efficient network security evaluation system, and provide more reliable technical guarantees for maintaining cyberspace security.

References

[1] Sun Mengmeng, Cao Chaoyang, Li Hongya. Research on Computer Network Security Technology Based on Deep Learning [J]. Information Recording Materials, 2024.

[2] Wang Yongliang, Tan Yuanbo, Zheng Xuetong. Research on Active Defense Strategy for Network Security Based on Deep Learning [J]. Industrial Information Security, 2024.

[3] Wu Junlei. Algorithm Optimization and Innovation of Deep Learning in Network Security Prediction and Analysis [J]. Software, 2024.

[4] Zhang Wei. Analysis of Computer Network Security Issues and Countermeasures - Review of "Computer Network Security Experiment Guide" [J]. Journal of China Safety Science, 2024.

[5] Yang Xing. Analysis of Security Maintenance Strategies in Computer Communication Networks [J]. Integrated Circuit Applications, 2024.

[6] [6] Zhao Yuan. Discussion on Computer Network Security Technology Based on Big Data [J]. Digital Communication World, 2024.

[7] Shen Yi. Computer Cryptography: Data Confidentiality and Security in Computer Networks [J]. Office Automation, 2024.

[8] Lei Xuefeng. Research on Computer Network Security Issues and Countermeasures [J]. Popular Science, 2024.

[9] Hu Zinan. Analysis of Computer Communication Network Security and Protection Strategy [J]. Science and Technology Information, 2024.

[10] Wu Jiacheng, Yu Xiao. A Review of Research on Network Security Risk Assessment Methods [J]. Electronic Science and Technology, 2024.

[11] Qian Feng. Research on Enterprise Network Security Operation Capability Evaluation [J]. Network Security and Informatization, 2024.

[12] Sun Yongjian. Application Analysis of Intelligent Computer Network Security Technology [J]. Information and Computer (Theoretical Edition), 2024.

[13] Lin Shuangqin. Design and Optimization of Network Security Defense System Based on Deep Learning [J]. Network Security and Informatization, 2024.

[14] Sun Min, Cheng Qian, Ding Xining. Android malware detection method based on CBAM-CGRU-SVM[J]. Journal of Computer Applications, 2024.