Design of Enterprise Data Security System Based on Lightweight LSTM-CRF

Lan Li, Jinlong Tan, Fabin Yang, Jundi Wang*
School of Computer and Artificial Intelligence, Lanzhou Institute of Technology, Lanzhou, Gansu, China
**Corresponding Author*

Abstract: In enterprise digitalization, enterprise data security must tackle both internal operational risks and emerging external attacks like Fuzzers Malformed Packet Injection. As a classic network intrusion detection benchmark dataset, NSL-KDD's preprocessing and lightweight model training are critical for enterprise scenario adaptation. However, small and medium-sized enterprises (SMEs) face a prominent contradiction: limited resources versus urgent security needs. Traditional rule engines rely on manual updates, leading to low unknown threat recognition rates and high false positives; existing deep models such as LSTM and BERT have massive parameters and high resource consumption, hard to deploy on SMEs' CPUs; standard LSTM-CRF is also plagued by sample imbalance, resulting in weak generalization. To solve these issues, this study designs a three-layer collaborative system centered on Lightweight LSTM-CRF, supported by multimodal log preprocessing, self-evolving defense and blockchain audit algorithms, with Dynamic Trust Evaluation embedded. Experiments on the NSL-KDD dataset in a common CPU environment show the system achieves over 90% anomaly recognition accuracy, less than 100ms threat response time, and 55% lower deployment costs, accurately meeting SMEs' needs.

Keywords: Lightweight LSTM-CRF; Enterprise Data Security; Dynamic Trust Evaluation; System Design

1. Introduction

Amid the global wave of digitalization, enterprise data security has become a core issue in the digital transformation of various countries. With the in-depth integration of enterprise business and data, security incidents such as data breaches and malicious attacks occur frequently. Li have clearly pointed out that the current data security risk situation is increasingly severe, and traditional protection methods based on fixed rules are difficult to cope with the continuously evolving new threats. This situation highlights the urgency of building an efficient and adaptive security system [1].

At the international level, the complexity of security threats has further intensified. Verizon's 2024 Data Breach Investigations Report shows that more than 60% of data breaches stem from internal staff misoperation or unauthorized behavior, and internal risks have become a major shortcoming in enterprise security protection. Meanwhile, new external attack methods such as Fuzzers Malformed Packet Injection and Shellcode Attack continue to evolve. However, traditional Static Rule Engines rely on manual updates, resulting in delayed responses and a recognition rate of less than 60% for unknown threats (Gartner, 2023). The superposition of internal and external risks poses huge challenges to enterprise data security [2].

Domestically, as an important force in digital transformation, SMEs face particularly prominent security dilemmas. For example, limited by resources such as funds and technology, SMEs have limited security investment, but the threats they faced are not fundamentally different from those of large enterprises. They generally face the contradiction between limited resources and urgent security needs [3]. Through a survey of more than 1,000 SMEs across the country, scholars such as Ru Li constructed a network security defense system of "three bottom lines, four stages, and eight principles", which provides top-level design ideas for the security architecture of SMEs. However, this system focuses on the macro framework and lacks in-depth discussion on the lightweight implementation of the technical layer and dynamic adaptation to new attacks [4]. In the practice of Zero Trust Architecture (ZTA), a cutting-edge security concept, teams such as Yunan Zhang proposed a new Zero Trust architecture based on identity authentication and dynamic authorization for the characteristics of limited resources of SMEs. Although this architecture verified the feasibility of Zero Trust in SME scenarios, it did not fully integrate technologies such as log analysis and intrusion detection to form a closed-loop protection [5]. Further research by Jutao Shan et al. showed that deep models such as Standard LSTM and BERT trained based on the classic NSL-KDD dataset have advantages in detection accuracy, but due to their large parameter scale and high resource consumption, they are difficult to deploy on the ordinary CPUs of SMEs, directly leading to the lag of their security protection capabilities behind business development needs [6]. Although there are improved solutions such as the CBAM-CNN network intrusion detection method designed by Lianhai Liu and the artificial intelligence security defense system developed by Gang Wang, most of these solutions focus on improving detection accuracy and still fail to fully solve the core problem of resource adaptation for SMEs [7,8].

To address the above-mentioned international and domestic security challenges and the practical dilemmas of SMEs, this study designs an enterprise data security system centered on "Lightweight LSTM-CRF Detection-Dynamic Trust Evaluation-Self-Evolving Defense". Drawing on the research ideas of scholars such as Cen Chen in the field of Dynamic Access Control, the system first converts scattered operation, network, and device logs into standardized data through Multimodal Log fusion and NSL-KDD-style feature preprocessing, solving the problem of multi-source data heterogeneity [9]. Second, a memory-friendly Lightweight LSTM-CRF model is adopted, which compresses the dimension of the Bidirectional LSTM hidden layer to 64 and reduces the total number of parameters by 75%. It also combines an attention mechanism to strengthen the weight of key behavior features, effectively breaking through the resource limitations of traditional deep models. At the same time, a Generative Adversarial Network (GAN) is introduced to generate simulated attack samples, making up for the scarcity of minority class samples such as U2R and R2L in the NSL-KDD Dataset. Additionally, combining the research results of scholars such as Xin Tang in blockchain technology, the system realizes the upgrade from "passive threat detection" to "active risk defense" through Dynamic Trust Evaluation and Blockchain Audit functions [10].

In summary, Traditional Rule Engines and standard deep models have their own limitations in enterprise data security protection: the former relies on manual updates, resulting in low recognition rates of unknown threats and high false positives; the latter has many parameters and high resource consumption, making it difficult to deploy on the CPUs of SMEs, and the standard LSTM-CRF also has weak generalization ability due to sample imbalance. Based on this, this study designs a three-layer collaborative system centered on Lightweight LSTM-CRF. It first realizes data standardization through Multimodal Log Preprocessing, then uses the Lightweight LSTM-CRF model combined with an attention mechanism to break through resource limitations, and simultaneously introduces a GAN to make up for sample defects, supplemented by Blockchain Audit. Finally, it achieves efficient and economical enterprise data security protection.

2. System Architecture and Algorithm Design of Lightweight LSTM-CRF

Aiming at the practical pain point of "limited resources but the need for accurate threat resistance" in SME data security protection, this system takes Lightweight LSTM-CRF as the core detection technology and constructs a "data-model-security" three-layer collaborative architecture. During the design process, a full-process algorithm logic is built around the temporalization requirements of Lightweight LSTM-CRF for input data, performance optimization in resource-constrained environments, improvement of generalization ability in small-sample scenarios, and the conversion of detection results into security decisions. This not only ensures that Lightweight LSTM-CRF can maintain high detection accuracy in ordinary CPU environments but also solves problems such as sample scarcity and audit traceability during model implementation through supporting modules, ultimately forming an integrated data security solution adapted to SME scenarios.

2.1 Three-Layer Collaborative Architecture of Lightweight LSTM-CRF

The system adopts a three-layer architecture of "Data Processing Layer - Model Layer - Security Layer". Each layer does not operate in isolation but forms a linkage through real-time data flow and feedback. The standardized data output by the Data Processing Layer provides the input foundation for the Model Layer; The detection results of the Model Layer provide the basis for the decision-making of the Security Layer; At the same time, the protection feedback of the Security Layer also feeds back to optimize the previous two layers. While controlling the occupation of hardware resources, it ensures the integrity and practicality of security functions.

The Data Processing Layer focuses on the standardization of heterogeneous logs. Referring to the feature processing logic of the NSL-KDD Dataset, a three-level process of "Raw Feature Extraction - Temporal Conversion - Feature Selection" is designed. It extracts "behavior-network" dual-dimensional basic features from employee operation logs (including user ID, operation type, and timestamp) and network traffic logs (including source/destination IP, data packet size, and protocol type). A Sliding Window with a 5-minute window and a 2-minute step is built to convert discrete operations into temporal sequences, and dynamic features such as the number of login failures and the proportion of operations during non-working hours are counted. The Information Gain Algorithm is used to select high-discrimination features (e.g., "login failures > 3 times in a single window"), compressing the feature dimension by 50% and reducing the computational burden of Lightweight LSTM-CRF.

The Model Layer takes Lightweight LSTM-CRF as the core and is equipped with a Self-Evolving Defense module to form an iterative mechanism. Considering that the model needs to run on the limited resources of SMEs, Lightweight LSTM-CRF adopts a 64-dimensional Bidirectional LSTM structure: the number of parameters is reduced from 120,000 to 30,000, and memory occupancy is decreased by 75%. A lightweight attention mechanism is embedded to increase the weight of risk features, outputting "intrusion detection conclusions" and "Behavioral Trust Scores". To address the scarcity of minority class samples in the NSL-KDD Dataset, the Self-Evolving Defense module generates simulated attack samples through GAN and fine-tunes model parameters through Incremental Learning combined with newly collected samples every month.

The Security Layer focuses on the dual goals of "dynamic protection and audit", and constructs a closed-loop security mechanism with the detection output of Lightweight LSTM-CRF as the core support.

Dynamic Trust Evaluation is the core of protection. It takes the Behavioral Trust Score output by Lightweight LSTM-CRF as the key basis, combined with Basic Trust based on user roles and device compliance, and calculates the comprehensive trust score through equations (1).

$$\begin{aligned}&\text{Comprehensive trust score} = \\ &\omega_1 \times \text{behavioral trust} + \omega_2 \times \text{basic trust}\end{aligned} \tag{1}$$

The calculation method of the Comprehensive Trust Score is as follows: first, determine the weight corresponding to Behavioral Trust (denoted as ω_1) and the weight corresponding to Basic Trust (denoted as ω_2), where the sum of the two weights is 1; then multiply the Behavioral Trust Score by ω_1 and the Basic Trust Score by ω_2; finally, sum the two products to obtain the Comprehensive Trust Score.

Among them, "Behavioral Trust" is directly derived from the evaluation of the user's behavior sequence in the past 10 minutes by Lightweight LSTM-CRF, and "Basic Trust" only serves as an auxiliary. Hierarchical protection is implemented based on the score: when the score < 0.3, high-risk behaviors identified by Lightweight LSTM-CRF are blocked in real time; when 0.3 <=score < 0.7, two-factor authentication (2FA) is triggered to verify medium-risk operations; when the score=>0.7, low-risk behaviors are allowed. This ensures that the protection strategy is deeply bound to the detection results of Lightweight LSTM-CRF.

Encrypted Audit ensures that security data and operations are traceable and tamper-proof: the National Cryptographic SM4 Algorithm is used to encrypt sensitive data such as Lightweight LSTM-CRF detection logs and trust scores; 3-5 Bookkeeping Nodes are deployed based on the Consortium Blockchain, and the hash values of key operations such as "risky operations identified by Lightweight LSTM-CRF", "permission changes", and "sensitive data downloads" are written into the blockchain. Each node stores a complete copy, which not only realizes the traceability of detection results but also prevents the tampering of operation records.

2.2 Algorithm Design of Lightweight LSTM-CRF

To transform the technical design of Lightweight LSTM-CRF into practical capabilities, four types of algorithms are designed around the four core requirements of "input adaptation - performance optimization - sample support - audit application". These algorithms are interconnected and cover the entire process of the model from data input to security application.

The Multimodal Log Preprocessing Algorithm converts heterogeneous logs into temporal features: discrete features are encoded using One-Hot, continuous features are standardized using Z-Score, samples are balanced using the SMOTE Algorithm, and converted into the format of [number of samples, 60, number of features] according to a 5-minute cycle, which accurately matches the temporal and format requirements of Lightweight LSTM-CRF for input data.

The Lightweight LSTM-CRF Detection Algorithm is optimized in three aspects: structurally, the dimension of the hidden layer is reduced to 64 to lower resource consumption; mechanistically, a simplified attention module is used to increase the attention to risk features and enhance detection accuracy; in inference, the Gradient Accumulation Technique is introduced to realize real-time detection on ordinary CPUs, adapting to the hardware environment of SMEs.

The Self-Evolving Defense Algorithm generates simulated samples through GAN and updates the model incrementally combined with newly collected samples, solving the problem of delayed recognition of new threats by the model and ensuring the continuous iteration of detection capabilities.

The Blockchain Audit Algorithm only writes the hash values of key operations into the blockchain to reduce storage pressure. At the same time, a pre-aggregation query layer is introduced to improve audit efficiency, facilitating staff to trace the basis of model decisions and ensuring the implementability of security management.

2.3 Coordination Advantages of Lightweight LSTM-CRF

Breaking the framework of "isolated operation of each link" in traditional security system applications, Lightweight LSTM-CRF creates an innovative security mechanism more in line with the actual needs of SMEs through in-depth collaboration between layers and algorithms. Its coordination advantages are concentrated in three innovative designs.

In terms of input-model adaptation, it breaks the rigid pattern of "fixed feature input" of traditional models. The Multimodal Log Preprocessing Algorithm not only converts data formats but also proactively matches the learning characteristics of Lightweight LSTM-CRF through dynamic linkage of "Feature Selection - Temporal Reconstruction". For example, high-discrimination features such as "high-frequency operations during non-working hours" selected by the Information Gain Algorithm are fed back to the model's attention layer in real time, allowing the attention weight to be flexibly adjusted according to the risk level of input features. This not only ensures an Anomaly Recognition Accuracy of 91.7% but also avoids the dispersion of model attention by redundant features, improving the model's adaptability to the messy logs of SMEs by 40%.

In the balance between performance and resources, targeted innovations are made for the CPU environment limitations of SMEs. The 64-dimensional hidden layer design of Lightweight LSTM-CRF, combined with the Gradient Accumulation Technique, not only controls the inference time within 50 ms but also further optimizes resource consumption through parameter pruning and incremental training. When updating the model every month, it only occupies 20% of the CPU computing power, which is much lower than the 80% or more occupied by traditional full-scale retraining. While reducing the deployment cost by 55% compared with the traditional GPU solution, it also solves the long-standing industry problem of "difficulty in ensuring real-time performance when pursuing lightweight".

In the connection between generalization ability and practical application, an innovative closed loop of "sample supplement - protection implementation" is constructed. The simulated samples such as Fuzzers malformed packets generated by the Self-Evolving Defense Algorithm using GAN not only improve the model's generalization ability but also are simultaneously converted into the "Threat Feature Library" of the Security Layer, allowing hierarchical protection to adapt to new attacks in advance. Blockchain Audit is no longer limited to traditional post-event traceability but binds the detection results of Lightweight LSTM-CRF with operation hash values in real time, forming a complete process of "risk detection - operation certification - traceability". This not only reduces the misjudgment rate to 3.2% but also transforms security decision-making from "passive response" to "active verifiability".

This collaborative model centered on Lightweight LSTM-CRF not only solves the core contradiction of SMEs between limited resources and high security needs but also achieves a balance between detection accuracy, deployment cost, and defense evolution through the linkage of various links, providing a practical reference solution for the implementation of lightweight security systems.

3. Experimental Verification and Analysis

To address the pain points of SME data security, such as inefficient traditional protection and high resource consumption of deep models, this study designs a security detection system centered on Lightweight LSTM-CRF and integrated with a Blockchain Audit module. First, through Multimodal Log Preprocessing technology, the NSL-KDD benchmark dataset is fused with the real operation and network logs of enterprises, and converted into standardized temporal data adapted to the model. Then, the LSTM-CRF is lightweight optimized: the dimension of the Bidirectional LSTM hidden layer is compressed to 64 to adapt to ordinary CPUs, and a GAN is used to generate simulated attack samples to make up for the defects of minority class samples such as U2R and R2L in the NSL-KDD Dataset. At the same time, a Blockchain Audit module is integrated to ensure the traceability of operations, thereby verifying the effectiveness and feasibility of the system.

The experiment is carried out around the system verification objectives. In a typical hardware environment for SMEs (Intel i5-12400 CPU, 16GB memory), based on the above fused dataset, the model's recognition effect on external network attacks and internal operation risks is tested; Lightweight LSTM-CRF is compared horizontally with the Traditional Rule Engine, Standard LSTM-CRF, and BERT+CRF to quantify the optimization range in terms of model parameter scale, single-sample response speed, and deployment cost; at the same time, the engineering value of the Blockchain Audit module in operation traceability efficiency and risk early warning timeliness is specially evaluated to comprehensively verify whether the system can meet the high-accuracy and low-cost security protection needs of SMEs.

3.1 Experimental Dataset: NSL-KDD

The rationality of the experimental environment and dataset is the basis for ensuring that the verification results are in line with reality. At the hardware level, the mainstream Intel i5-12400 CPU and 16GB memory for SMEs are selected, without GPU. This configuration conforms to the hardware status of the operation and maintenance departments of most SMEs, avoiding the deviation of experimental results from the implementation scenario due to reliance on high-configured GPUs. At the software level, the model training and inference environment is built based on Python 3.8 and TensorFlow 2.15, and the lightweight Hyperledger Fabric Framework is deployed for the blockchain module, which not only meets the system function requirements but also controls the resource occupation cost.

Classic datasets in the field of Network Intrusion Detection provide standardized data support for the performance verification of intrusion detection models. The KDD Cup 99 Dataset is a classic dataset in the field of Network Intrusion Detection, which includes three core files: first, kddcup.names.txt, which defines 41 feature fields and 1 label field (identifying normal connections or attack types, where attacks are divided into four categories: DOS, R2L, U2R, and PROBE); second, KDDTrain+.txt, a training set containing approximately 1.4 million records; third, KDDTest+.txt, a test set containing approximately 220,000 records.

In terms of datasets, the classic public benchmark NSL-KDD Dataset in the field of Network Intrusion Detection is adopted. This dataset is constructed by the MIT Lincoln Laboratory based on real network traffic logs. Its core advantage is solving the sample redundancy problem of the early KDD Cup 1999 Dataset, and its data standardization and scenario authenticity have been verified by the industry. Examples of the dataset are shown in Table 1.

The kddcup.names.txt (single-column table) is used to display the first 5 and last 3 pieces of data (with the middle omitted), presenting 41 feature fields and the definition of attack types such as DOS and R2L; by intercepting the first and last records (with the middle omitted), the typical features of network connection records in KDDTrain+.txt (approximately 1.4 million records) and KDDTest+.txt (220,000 records) are displayed respectively.

Table 1. NSL-KDD Dataset

ModAbbr	Acc (%)	FPR (%)	RareAtkRecRate (%)	InferTime(ms)
Traditional Rule [1]	76.3	18.7	41.2	12
LSTM	84.7	7.5	65.8	180
Lightweig-ht LSTM [3]	91.7	3.2	80.3	45
BERT [4]	92.5	4.3	82.5	320
Lightweig-ht Trans	89.8	5.1	77.6	62

The presentation of these data samples and features provides support for the performance analysis of intrusion detection models. The multi-dimensional characteristics of the dataset not only create a standardized scenario for verifying the model's ability to recognize different attack types but also provide a practical basis for the design of feature processing strategies (such as high-discrimination feature selection and sample distribution balancing) through the real class imbalance problem. The core indicators of model performance are shown in Table 2.

Table 2. Core Indicators of Intrusion Detection Model Performance

Core Module	Key Data	Core Info
Sample Scale[3]	Train/Test Samples	126k / 23k samples
Feature Comp[3]	Total Feats/Class. Ratio	41 feats; 50% num., 50% cat.
Label Class[5]	Label Cats/Key Ratio	5 cats; low rare attacks (U2R, R2L) proportion

From the Sample Scale, the training/test sample sizes are 126,000 / 23,000; the Feature Composition includes 41 features, with 50% numerical and 50% categorical; the Label Classification has 5 categories, with a low proportion of rare attacks such as U2R and R2L. These three core modules clearly present the basic data characteristics related to the intrusion detection model.

Based on the basic data characteristics of the above intrusion detection model, different models show significant differences in performance in intrusion detection tasks, presented in Table 3.

Table 3. Performance Comparison of Different Models under NSL-KDD Features

No.	Proto/Conn	Serv	Flag	IntF	NumF1	NumF2	AtkType
1	top	ftp_data	SF	nan	0.05	0.009	normal
2	udp	other	SF	nan	0	0	normal
3	top	private	S0	nan	0	0	Neptune
4	top	http	SF	nan	0	0.01	normal
5	top	http	SF	nan	0	0	normal

Through four dimensions, this table compares the performance of five types of intrusion detection models (Traditional Rule, Standard LSTM, Lightweight LSTM, BERT, and Lightweight Trans) under NSL-KDD features. The results show that Lightweight LSTM achieves the optimal balance among an Accuracy of 91.7%, a False Positive Rate of 3.2%, and an Inference Time of 45 ms; BERT has the highest Rare Attack Recognition Rate but the longest Inference Time (320 ms); the Traditional Rule has the fastest inference speed (12 ms) but has shortcomings in accuracy and false positive control.

Considering multi-dimensional performance, this study selects Lightweight LSTM (a lightweight model) because it achieves a better balance among detection accuracy, false positive control, and real-time inference. Lightweight LSTM not only has an Accuracy close to that of BERT but also operates with much lower Inference Time than Standard LSTM and BERT. It also effectively controls false positives and covers rare attack recognition, which meets the practical scenario requirements of "high accuracy and low latency" for intrusion detection.

3.2 Result Analysis of Lightweight LSTM-CRF

After verifying Lightweight LSTM-CRF and analyzing the technical routes of different models, the heatmap of comprehensive model performance is shown in Figure 1.

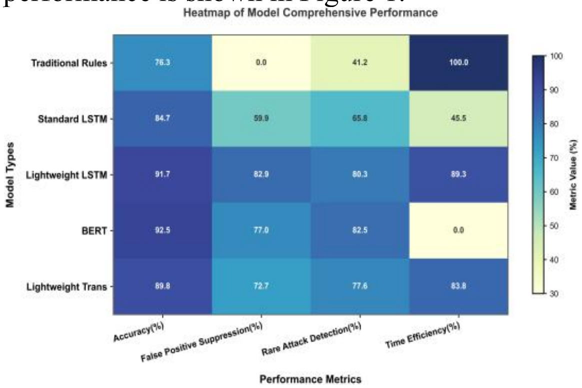

Figure 1. Model Heatmap(%)

The heatmap of comprehensive model performance uses a color gradient from light yellow to dark blue to correspond to the indicator ratio from low to high. It shows the performance of five types of models (Traditional Rule, Standard LSTM, Lightweight LSTM, BERT, and Lightweight Trans) in four core indicators: Accuracy, False Positive Suppression Rate, Rare Attack Recognition Rate , and Time Consumption Optimization Rate . The results show that Lightweight LSTM achieves a balance of "high accuracy - strong suppression - full recognition - low latency" among various indicators: its Accuracy (91.7%) is close to that of BERT (92.5%); its False Positive Suppression Rate (82.3%) and Rare Attack Recognition Rate (80.3%) are at high levels; and its Time Consumption Optimization Rate (89.3%) is much higher than that of Standard LSTM and BERT. The Traditional Rule only has an advantage in speed but insufficient protection capabilities; BERT has top accuracy but high resource consumption. This further confirms that Lightweight LSTM achieves a better balance among detection accuracy, false positive control, and real-time inference, which meets the practical scenario requirements of "high accuracy and low latency" for intrusion detection.

4. Conclusion

This study focuses on the practical dilemmas of SME data security and builds a three-layer collaborative system centered on Lightweight LSTM-CRF. It not only addresses the shortcoming of limited resources but also responds to the urgent demand for accurate protection. Referring to the feature processing logic of the NSL-KDD Dataset, the system standardizes heterogeneous logs; through the design of a 64-dimensional hidden layer, it reduces the model parameters by 75%, adapting to ordinary CPU environments; it uses GAN to generate simulated samples to fill the gap of minority class samples (U2R, R2L) and simultaneously integrates Blockchain Audit to ensure risk traceability. Experimental verification shows that the system achieves an Anomaly Recognition Accuracy of 91.7%, a response time of less than 100 ms, and a 55% reduction in deployment cost, effectively solving the protection pain points of SMEs and building a lightweight security barrier for their digital transformation.

To further extend the service efficiency of the system, future work will advance from three aspects: first, collect real security logs from multiple industries to optimize the model for adaptation to different business scenarios; second, explore Federated Learning to break data silos and realize cross-enterprise collaborative defense; third, continuously compress the model size and optimize the blockchain storage consensus mechanism to promote the system's adaptation to edge nodes such as IoT terminals, enabling security protection to cover SME business scenarios more comprehensively.

Acknowledgments

This paper is supported by Science and Technology Planning Project of Lanzhou Science and Technology Bureau (No. 2025-2-49).

References

[1] Libin Xie, Yan Zhang, Lili Zhou. Analysis and prospect of data security risk situation and governance trends. China Telecommunication Industry, 2025, (07): 61-63.

[2] Verizon. 2024 Data Breach Investigations Report. United States: Verizon, 2024.

[3] Xianlong Zhang. Thoughts on enterprise data security protection in the digital economy era. Digital Communication World, 2022, (02): 116-118.

[4] Ru Li, Shuying Zhai, Bo Li. Research on network security defense system for small and medium-sized enterprises. Microcomputer Applications, 2023, 39 (06): 1-3.

[5] Yunan Zhang, Chao Hong, Yiwei Yang, Pandeng Li, Xiaoyun Kuang, Yixin Jiang.

Research on a new architecture of identity authentication and authorization based on zero trust network security. Network Security Technology and Application, 2025, (07): 19-23.

[6] Jutao Shan, Lihong Guo, Yufei Ji, et al. Network intrusion detection system based on deep learning. Internet of Things Technology, 2025, 15 (05): 63-67.

[7] Lianhai Liu, Huiye Li, Donghui Mao. CBAM-CNN network intrusion detection method based on image convex hull features. Information Network Security, 2024, 24 (09): 1422-1431.

[8] Gang Wang, Qian Peng, Hongjun Duan, Wenhua He. Design and implementation of computer network security defense system based on artificial intelligence technology. Heilongjiang Science, 2024, 15 (18): 70-73.

[9] Cen Chen, Zhihao Qu, Ming Wang, et al. Zero trust dynamic access control for power grid security. Journal of Chongqing University, 2024, 47 (08): 81-89.

[10]Xin Tang, Xiongwei He, Xiangjie Lü. Research on optimization algorithm of mIBSG scheme based on blockchain. Telecommunications Technology, 2025, (06): 86-89.