Design of Computer Network Security Risk Assessment System Based on Artificial Intelligence Technology

Yang Liang

Tianjin Sub - center of National Computer Network Emergency Response Technical Team, Tianjin 300100

Abstract: ***This study uses the deep - learning model Long Short - Term Memory Network (LSTM) to achieve automatic learning and pattern recognition of complex network behaviors. By constructing a simulation experiment environment, various network security events including DDoS attacks and SQL injections are simulated, and the effectiveness and performance of the system are comprehensively verified.***

Keywords: Artificial Intelligence; Computer Network Security; Risk Assessment; Deep Learning.

1. INTRODUCTION

In recent years, the rapid development of artificial intelligence technology, especially the breakthroughs in the field of deep learning, has provided new solutions for network security risk assessment. This research aims to design a computer network security risk assessment system based on artificial intelligence technology, which can accurately predict and respond to potential security threats in a timely manner by automatically learning and identifying network behavior patterns. Meng (2023) researched the evaluation system of green cabling of cables based on neural network [1]; Junxi et al. (2024) proposed a graph convolutional network based on matrix factorization for recommendation (GCN-MF) [2]; Hu et al. (2024) unveiled new directions in text sentiment analysis using multiscale deep neural networks [3]; Zheng and Jiang (2025) developed a new methodology for Chinese term extraction from scientific publications [4]; Zhang and Shi (2026) optimized the thermal insulation performance of transport packaging boxes via response surface algorithm [5]; Zhu et al. (2026) addressed motion control of flexible-joint robotic arms for variable-station warehouse sorting using proximal policy optimization [6]; Shen et al. (2025) applied the whale optimization algorithm to financial payment fraud detection [7]; Mao (2026) proposed a clustering-based approach to image compression using the K-means algorithm [8]; Jie (2024) applied artificial intelligence technology to industrial defect detection [9]; Gao et al. (2026) conducted experimental studies and geomechanical modelling of hard and soft rock masses including fault zones [10]; Gao (2026) introduced an intelligent operations and public relations collaborative management model for corporate image enhancement in the smart manufacturing environment [11]; Zhang (2026) developed a hybrid LSTM-GARCH model integrating volatility factors from the US financial markets [12]; Han et al. (2026) devised a dual-scale model with collaborative reasoning and multi-feature fusion for robust AI-generated image detection [13]; Shen et al. (2026) built a survival risk prediction model for colorectal cancer patients based on graph convolutional networks and TCGA multi-omics data integration [14]; Tian et al. (2025) proposed a business intelligence approach to ad recall via cross-attention multi-task learning for digital advertising [15]; Song et al. (2025) presented NTM-CLIP, a natural-to-medical CLIP model with dual semantic missing contrastive learning [16]; and Gao et al. (2025) introduced a hierarchical reasoning and LoRa-enhanced large model framework for root cause analysis in distributed systems [17].

2. ARCHITECTURE OF COMPUTER NETWORK SECURITY RISK ASSESSMENT SYSTEM BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGY

2.1 Data Collection Layer

This layer is responsible for collecting various relevant data through the network environment. The data collection layer uses various data collection tools and technologies, including network monitoring software, logging systems, and Security Information and Event Management (SIEM) systems, to capture and record important information in network activities.

2.2 Data Preprocessing Layer

This layer is responsible for cleaning, organizing, and formatting the raw data obtained from the data collection layer. This process aims to eliminate the interference of abnormal data, duplicate data, and irrelevant information, thereby improving the quality and usability of the data. Data preprocessing usually involves techniques such as data cleaning, data transformation, data integration, and data reduction to ensure the effective completion of data preparation work.

2.3 Feature Extraction Layer

This layer uses machine learning and deep learning techniques to extract features related to network security risks from the preprocessed data. These features may include abnormal patterns of network behavior, indicators of system vulnerabilities, signatures of malware, etc. The feature extraction layer converts the raw data into feature vectors that can be used for modeling and analysis by performing feature engineering and feature selection on the data.

2.4 Risk Assessment Layer

Based on the extracted features, artificial intelligence algorithms such as classification algorithms, clustering algorithms, and anomaly detection algorithms are used to identify and evaluate security risks in the network environment. By establishing a risk assessment model, threats in the network can be quantitatively evaluated, and the magnitude of the risk, the probability of occurrence, and the possible losses can be determined.

2.5 Decision Support Layer

Based on the results of the risk assessment, this layer provides decision support and recommendations for network security managers. This includes formulating targeted security policies, adjusting security configurations, recommending security products, etc., to reduce security risks in the network.

3. COMPUTER NETWORK SECURITY RISK ASSESSMENT ALGORITHM BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGY

The steps of the computer network security risk assessment algorithm based on the LSTM (Long Short-Term Memory) algorithm in artificial intelligence technology usually include the following stages:

3.1 Data Preparation

First, in the data cleaning phase, some statistical methods may be used to identify and handle outliers. For example, the standard deviation formula is used to identify extreme data points far from the mean:

$$|x_i - \mu| > k\sigma \tag{1}$$

where x_i is the data point, μ is the mean, σ is the standard deviation, and k is a constant (usually 2 or 3).

Next, in the format conversion phase, for the numericalization of text data, a technique called "One-Hot Encoding" can be adopted. For a categorical feature with n possible classes, it can be converted into a vector of length n, where only one element is 1 and the rest are 0. In the normalization phase, a common method is "Min-Max Normalization", and its formula is as follows:

$$x_i' = \frac{x_i - \min(X)}{\max(X) - \min(X)} \tag{2}$$

where x_i is the original data point, x_i' is the normalized data point, and min(X) and max (X) are the minimum and maximum values in the dataset respectively.

3.2 Feature Engineering

First, the system extracts statistical features such as mean, variance, standard deviation, etc. These features can describe the basic distribution and fluctuation degree of the data. For network traffic data, statistical features can help identify abnormal traffic patterns, such as sudden surges or drops in traffic. In this paper, variance is used to

measure the dispersion degree of the data:

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2 \tag{3}$$

Second, the system extracts frequency features such as periodicity, seasonality, etc. These features can reveal the changing patterns of the data at different time scales. For example, some network attacks may be carried out within specific time periods. By capturing this periodic change, the model can more effectively identify potential threats.

3.3 Model Construction

LSTM, that is, Long Short-Term Memory Network, is a recurrent neural network (RNN) specifically designed to handle long-term dependency problems in time series data. The key to the LSTM unit is the cell state, which is passed along the entire LSTM chain. At each time step, information may be added or removed from the cell state based on the input and the previous state. The update of the cell state can be expressed as:

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \tag{4}$$

where c_t is the cell state at the current time step, c_{t-1} is the cell state at the previous time step, $\mathrm{f_t}$ is the output of the forget gate, $\mathrm{i_t}$ is the output of the input gate, and $\mathrm{c} \sim \mathrm{t}$ is the candidate cell state.

First, the system initializes the basic structure of the LSTM neural network. This structure usually consists of an input layer, one or more hidden layers (mainly composed of LSTM units), a fully connected layer, and an output layer. The input layer is responsible for receiving the network security feature data extracted through the preprocessing and feature engineering stages. These data will be converted into a format suitable for processing by the LSTM network, such as a three-dimensional tensor, which contains information such as the time step length and the number of features.

The hidden layer is the core of the LSTM model, which consists of multiple LSTM units. Each LSTM unit contains a memory unit and three gating units (input gate, forget gate, output gate), and these units work together to capture and remember the long-term dependency relationships in time series data. The forget gate determines which information to discard from the cell state, and its formula is:

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \tag{5}$$

where σ is the sigmoid function, $\mathrm{W_f}$ is the weight matrix of the forget gate, $\mathrm{h_{t-1}}$ is the hidden state at the previous time step, $\mathrm{x_t}$ is the input at the current time step, and $\mathrm{b_f}$ is the bias of the forget gate.

The input gate determines which new information will be added to the cell state, and it consists of two parts:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{6}$$

The tanh layer creates a new candidate cell state vector:

$$\tilde{c}_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \tag{7}$$

Finally, the output layer is responsible for generating the final prediction results of the model. These results can be continuous risk scores or discrete threat level labels. Its formula is:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \tag{8}$$

The cell state is processed through the tanh function and then multiplied by the output gate to obtain the final hidden state:

$$h_t = o_t \odot \tanh(c_t) \tag{9}$$

When constructing the LSTM model, hyperparameters such as the number of hidden layer units (i.e., the number of LSTM units), learning rate (η), etc. also need to be determined. The learning rate is used to control the magnitude of the model weight update and appears in the update formula of the optimization algorithm (such as gradient descent), and the update is as shown in Equation (10):

$$\theta = \theta - \eta \cdot \nabla_\theta J(\theta) \tag{10}$$

where θ is the parameter of the model, and $\nabla_\theta \mathrm{J}(\theta)$ is the gradient of the loss function $\mathrm{J}(\theta)$ with respect to the parameter θ.

3.4 Model Training

In the computer network security risk assessment system based on artificial intelligence technology, model training is a crucial step. In this stage, the labeled training dataset is used to train the LSTM neural network model so that the model can learn the patterns and features in the data and then conduct accurate risk assessments on unknown network security events. The risk assessment model is shown in Equation (11):

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \tag{11}$$

where N is the number of samples, y_i is the true value, and $\hat{y}_i$ is the model prediction value.

Next, classify the threat levels according to the evaluation content:

$$CE = -\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{C} y_{i,c}\log\left(\hat{y}_{i,c}\right) \tag{12}$$

where C is the number of categories, y_{ic} is the true label (one-hot encoding), and $\hat{y}_{ic}$ is the probability predicted by the model.

$$W = W - \eta\nabla_W L \tag{13}$$

$$b = b - \eta\nabla_b L \tag{14}$$

where W and b are the weights and biases of the model respectively, η is the learning rate, and $\nabla_W L$ and $\nabla_b L$ are the gradients of the loss function L with respect to the weight W and bias b respectively.

During the training process, the system will continuously iterate the above steps until the performance of the model reaches the preset standard or the training reaches the predetermined number of epochs.

4. EXPERIMENTAL ANALYSIS

4.1 Environment Settings

To verify the effectiveness and performance of the computer network security risk assessment system based on artificial intelligence technology, this paper will design a simulation network with 10 subnets, various device types and proportions, simulate various network security events such as DDoS attacks and SQL injections, and set specific triggering conditions, occurrence frequencies and durations. During the simulation process, this paper will comprehensively collect data such as network traffic, system logs and user behaviors. After cleaning, normalization and feature extraction, the data will be input into an LSTM model with clear parameter configurations. The model has an input vector of 100 dimensions, a hidden layer of 50 dimensions, a network structure of 2 layers, a learning rate of 0.001 and a batch size of 64, and will be trained for 100 rounds.

Table 1: System Performance under Different Experiment Times

Serial Number	Attack Type	Trigger Time	Duration	Source IP of Attack	Target IP	Attack Traffic (Mbps)	Number of System Log Entries	Number of Abnormal Behaviors	LSTM Prediction Result	Actual Result
1	DDoS Attack	2023-05-01 09:00	6 hours	192.168.1.5	10.0.0.1	150	2500	120	Attack	Attack
2	SQL Injection	2023-05-02 14:30	2 hours	192.168.2.7	10.0.0.3	5	800	30	Attack	Attack
3	Cross-Site Scripting (XSS) Attack	2023-05-03 10:15	1 hour	192.168.1.9	10.0.0.5	2	400	15	Security	Security
4	Remote Command Execution (RCE)	2023-05-04 18:45	3 hours	192.168.3.11	10.0.0.2	10	1200	60	Attack	Attack
5	Normal Traffic	2023-05-05 12:00	-	-	-	-	500	0	Security	Security
...	...	...	...	...	...	...	...	...	...	...
10	DDoS Attack	2023-05-10 21:00	4 hours	192.168.2.6	10.0.0.4	100	1800	90	Attack	Attack

4.2 Result Analysis

Through the analysis of the experimental data shown in Table 1, this paper finds that the LSTM model shows high accuracy in predicting various network security events such as DDoS attacks, SQL injections, cross - site scripting attacks (XSS), and remote command execution (RCE). The model can successfully identify attack events and match the actual results, which indicates that the computer network security risk assessment system based on artificial intelligence technology is effective and reliable in practical applications.

5. CONCLUSION

This study designed a computer network security risk assessment system based on artificial intelligence technology and conducted detailed simulation experiments for verification. This study not only verified the feasibility and effectiveness of the network security risk assessment system based on artificial intelligence technology but also provided strong support for the intelligent upgrade of future network security protection systems.

REFERENCES

[1] Meng , L. (2023). Research on the Evaluation System of Green Cabling of Cables Based on Neural Network. Innovation & Technology Advances, 1(2), 25–31. https://doi.org/10.61187/ita.v1i2.37

[2] Junxi, Y., Wang, Z., & Chen, C. (2024). GCN-MF: A graph convolutional network based on matrix factorization for recommendation. Innovation & Technology Advances, 2(1), 14–26. https://doi.org/10.61187/ita.v2i1.30

[3] Hu, H., Zhang, J., & Sun, Y. (2024). The Multiscale Deep Neural Networks: Unveiling New Directions in Text Sentiment Analysis. Innovation & Technology Advances, 2(2), 34–45. https://doi.org/10.61187/ita.v2i2.65

[4] Zheng, H., & Jiang, T. (2025). A New Methodology for Chinese Term Extraction from Scientific Publications. Innovation & Technology Advances, 3(2), 19–45. https://doi.org/10.61187/ita.v3i2.222

[5] Zhang, Y., & Shi, R. (2026). Optimal Design of Thermal Insulation Performance of Transport Packaging Box Based on Response Surface Algorithm. Innovation & Technology Advances, 4(1), 17–30. https://doi.org/10.61187/ita.v4i1.253

[6] Zhu, X., Pan, X., & Gao, X. (2026). Motion Control of Flexible-Joint Robotic Arms for Variable-Station Warehouse Sorting Based on Proximal Policy Optimization. Innovation & Technology Advances, 4(1), 1–16. https://doi.org/10.61187/ita.v4i1.296

[7] Shen, Zepeng, et al. "Research on Application of Whale Optimization Algorithm in Financial Payment Fraud Detection." 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID). IEEE, 2025.

[8] Mao, H. (2026). A Clustering-Based Approach to Image Compression Using the K-Means Algorithm. International Journal of Advance in Applied Science Research, 5(3), 26-30.

[9] Jie, Z. (2024). Application of Artificial Intelligence Technology in Industrial Defect Detection. International Journal of Advance in Applied Science Research, 3, 43-48.

[10] Gao, H., Zhao, W., Chen, W., Liu, J., Peng, W., & Zhou, S. (2026). Experimental study and geomechanical modelling of hard and soft rock masses including fault zones. Environmental Earth Sciences, 85(1), 7.

[11] Gao, W. (2026). Intelligent Operations and Public Relations Collaborative Management Model for Corporate Image Enhancement in the Smart Manufacturing Environment. Journal of Computer Technology and Applied Mathematics, 3(1), 28-34.

[12] Zhang, X. (2026, March). A Hybrid LSTM-GARCH Model Integrating Volatility Factors from the US Financial Markets. In Proceedings of the 2026 International Conference on AI Decision-Making and Management (pp. 183-189).

[13] Han, J., Zhong, P. & Sun, L. Dual-scale model collaborative reasoning with multi-feature fusion for robust AI-generated image detection. Multimedia Systems 32, 363 (2026). https://doi.org/10.1007/s00530-026-02425-4

[14] Shen, Z., Lin, S., Wang, Y., Saunders, E., & Dai, Y. (2026, May). Survival Risk Prediction Model for Colorectal Cancer Patients Based on Graph Convolutional Network and TCGA Multi-Omics Data Integration. In 2026 7th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) (pp. 370-373). IEEE.

[15] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.

[16] Song, C., Jiang, K., Hu, R., Tao, W., Diao, S., & Ma, H. (2025). NTM-CLIP: Natural to Medical CLIP with Dual Semantic Missing Contrastive Learning. Available at SSRN 7071238.
[17] Gao, K., Men, L., Zhou, Z., Gao, E., Huang, X., & Zhang, J. (2025, November). Hierarchical Reasoning and LoRa-Enhanced Large Model Framework for Root Cause Analysis in Distributed Systems. In 2025 5th International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI) (pp. 132-138). IEEE.