
Optimized LSTM-Informer Model for Accurate Detection of Network Threats in Hospital Environments

Hanteng Liu^{1,*}, Zonggeng Chen¹, Yishun Xia¹,
Siqu Qiao¹ and Jiayu Ou²

¹*Center for Information Technology & Statistics, Network Management Section,
The First Affiliated Hospital, Sun Yat-sen University, Guangzhou 510000, China*

²*Guangzhou Zhongke Mingnuo Data Co. Ltd, Guangzhou 510660, China*

E-mail: HantengLiu@outlook.com; foryouforme_m@163.com;

yal0858@gmail.com; cheesebrat@163.com; 13929563330@139.com

**Corresponding Author*

Received 08 April 2026; Accepted 31 May 2026

Abstract

In view of the complex hospital network environment, massive redundancy of security alarms, and lag in identification of real threats, this study proposes a hospital network security alarm model based on optimized Long Short-Term Memory (LSTM)-Informer. First, an attention-enhanced multi-dimensional alarm feature fusion module is constructed to integrate device logs, traffic data, and threat intelligence unique to hospital networks. Second, a hybrid bidirectional LSTM (BiLSTM) and improved Informer structure is designed to enhance long-range correlation mining and short-term burst alarm detection. The sparse attention mechanism is optimized with hospital threat-level priors to improve detection accuracy and reduce false alarms. The results show that among long-term correlation alarm types, the recall rate of port scanning, intranet lateral movement, and ransomware behavior are all $\geq 94.5\%$, and the false alarm rate is $\leq 2.8\%$, proving that the model effectively

Journal of Cyber Security and Mobility, Vol. 15.5, 1181–1210.

doi: 10.13052/jcsm2245-1439.1552

© 2026 River Publishers

filters redundant alarms in long-term sequences. Among the short-term burst alarm types, the F1 score of malicious traffic injection and data leakage attempts is $\geq 93.8\%$. Since the characteristics of phishing emails are more subtle, the false positive rate is slightly higher (4.0%), but it is still far lower than the traditional LSTM model (10.8%). The performance of the optimized model is significantly improved compared with the traditional model, and it can effectively alleviate the alarm fatigue of security operation personnel. This study provides an efficient alarm research and judgment solution for hospital network security intelligent operation and maintenance, helping to achieve active defense.

Keywords: Hospital, network security, informer, network security alarm, long short-term memory.

1 Introduction

With the frequent emergence of new threats such as attacks and ransomware, the number of hospital Network Security Alarms (NSA) grows explosively. A top-level hospital generates nearly 100,000 alerts per month. The False Alarm Rate (FAR) is as high as more than 30%, causing security operations personnel to fall into “alarm fatigue” [1]. Hospital networks carry sensitive electronic medical records and service systems and face severe and uncontrollable cyber threats. With the spread of ransomware and emerging attacks, security alerts grow explosively, with a FAR exceeding 30%, leading to severe alert fatigue and delayed threat response. Traditional methods rely on static rules and show low effectiveness against variant or unknown threats, while multi-source data integration and long-term trend analysis are insufficient [2]. Long Short-Term Memory (LSTM) models capture temporal dependencies but suffer from gradient vanishing in long sequences. Informer improves long-sequence efficiency via ProbSparse attention but lacks sensitivity to short-term burst alarms. Given hospital alerts exhibit both long-term continuity and short-term burstiness, a single model cannot effectively extract both features, creating an urgent need for a fused optimization model [3].

Considering the above, the main contributions of this work are as follows:

- An attention-enhanced multi-dimensional alarm feature fusion mechanism is proposed for hospital-specific network scenarios: This mechanism integrates heterogeneous data from hospital network devices (firewalls, medical device gateways, Digital Imaging and Communications

in Medicine (DICOM) servers), and adopts improved Z-score standardization and dynamic attention weight allocation. It effectively solves the problem of key threat feature dilution caused by multi-source data heterogeneity in hospital networks.

- A BiLSTM-Improved Informer hybrid coding structure is designed to balance long-term dependence and short-term burst characteristics: The structure uses BiLSTM to capture short-term burst threat features and optimizes the Informer's ProbSparse attention mechanism by introducing hospital network threat level prior information.
- Domain-adaptive optimization strategies are integrated into the model training process: Focal Loss is used to alleviate the category imbalance problem of hospital alarm data (a small number of real threat samples), and adaptive sparse attention with hospital threat priors is designed.
- A complete hospital network threat detection and alarm research and judgment scheme is formed: The model is verified by actual hospital alarm data and classic state-of-the-art (SOTA) datasets, effectively reducing the FAR of hospital NSAs and providing a feasible technical solution for the intelligent operation and maintenance of hospital network security.

This research is of critical importance for hospital network security, as health-care systems carry sensitive patient data and require stable and real-time medical services. The proposed method improves existing knowledge and practice in three key aspects. First, it overcomes the limitation that traditional deep learning models can only handle either long-term continuous threats or short-term burst alarms, but not both, thus filling the gap in temporal feature adaptation. Second, it challenges the conventional practice of using generic time-series models for hospital alarm detection, and instead provides a domain-adaptive design with hospital threat priors that better fits medical network characteristics. Third, it reduces the extremely high FAR that has long troubled security operators, moving from passive rule-based filtering to intelligent and active threat identification. By integrating feature fusion, optimized attention, and hybrid modeling, this study offers a practical and reliable solution for real-world hospital security operation and maintenance.

The remainder of this paper is organized as follows. Section 2 focuses on the hospital NSA model designed this time based on optimized LSTM-Informer, which is also the focus and innovation point of this research. Section 3 details the analysis of experimental data results. Section 4 draws conclusions based on the experimental results, elaborating on the flaws of

this design and the directions that require further in-depth research in the future.

2 Related Work

In recent years, the application of deep learning in the field of NSA analysis has become a research hotspot. Currently, network security incidents occurred frequently. Malware proliferation, network attacks, data leaks, and other issues posed threats to hospital network security, and effective alarm solutions were urgently needed. Liu et al. conducted an in-depth analysis of the current status of network security and proposed monitoring and early warning strategies and strengthening measures to provide support for hospitals to deal with related security risks [4]. Security Information and Event Management (SIEM) platforms had problems such as inefficient alarm management and insufficient integration with real-time communication tools in hospital scenarios. Therefore, Shankar et al. built the Adrian system to integrate SIEM functions with a real-time collaboration platform, and conducted a case study using Wazuh integrated with Slack. This result enabled functions such as real-time alarm distribution, improved the hospital's NSA response efficiency, and could be combined with AI to further optimize alarm priority and response automation [5]. The large number of alarms in the Network Intrusion Detection System (NIDS) was difficult to prioritize, and the deep learning model lacked transparency. Kalakoti et al. used TalTech's real NIDS alarm dataset to develop an LSTM model to rank alarms, compared four explainable AI methods, and evaluated them from multiple dimensions. DeepLIFT performed best, and its obtained features were highly consistent with the key features identified by Security Operations Centers (SOC) analysts, providing support for optimizing hospital NSA models [6]. In response to the problem of analyst alert fatigue caused by the proliferation of security incidents in SOC, Jalalvand et al. reviewed the standards and methods of Alert Prioritization (AP) in SOC. They analyzed the advantages and disadvantages of various AP solutions based on HumanAI teamwork and took into account automation, enhancement, and collaboration, and clarified future research areas to provide support for AP technology advancement and SOC's more efficient response to security incidents [7].

In response to the serious threats to hospital network security, Huang et al. adopted a multi-layer protection equipment deployment solution such as intrusion detection and firewalls. This solution monitored network traffic in real-time through the model, identified abnormal behaviors, realized early

warning, interception, and alarm of potential attacks, ensured the stable operation of the hospital network system, and provided guidance for the improvement of hospital network security operations [8]. In view of the threats to hospital network security, an intelligent alarm system needed to be developed to ensure security. Zuberi and Ahmad collected relevant data based on integrated IoT sensors and analyzed and detected anomalies through machine learning algorithms. Its suspicious behavior detection accuracy of 91.12% was higher than existing systems, could provide real-time alarms, shorten security response time, and provide reference for subsequent research and development of related intelligent security systems [9]. NIDS in hospital networks was prone to generate a large number of low-importance alarms. Existing machine learning methods were difficult to screen efficiently, and active learning was insufficiently applied in this field. Vaarandi and Guerra-Manzanares studied the application of active learning technology in NIDS alarm classification, filling the relevant research gaps and providing an effective solution for accurately screening high-importance alarms [10]. There were problems in hospital NSA, such as false positives and missing exceptions caused by the high dimensionality and high noise of multivariate time series, and ignoring the correlation of different timestamp states. Huang et al. fused relevant network structures to capture features and continuous correlations, optimized dual modules, and verified on a benchmark dataset that its performance was better than existing methods, with an accuracy increase of up to 2%. It could efficiently detect anomalies and locate attack points [11]. To solve the needs of hospital network intrusion detection and improve the adaptability and accuracy of NIDS in dynamic environments, Elezmazy and Mostafa used network traffic statistics to build an LSTM-based autoencoder model to capture time dependence. This model achieved effective distinction between normal and intrusive activities. The model accuracy, precision, and other indicators reached 99.7–99.9%, fully verifying its effectiveness and flexibility in hospital NSA [12].

To sum up, for hospital NSA, researchers have some involvement and research in intrusion detection, machine learning algorithms, autoencoders, and data identification. However, existing research has not yet addressed the issues of “balancing long-term dependence and short-term burst characteristics”, “multi-source heterogeneous data fusion”, and “balancing low FAR and high recognition rate” of hospital alarm data. Therefore, to address the key technical problems in hospital NSA research and judgment, this study proposes an optimized LSTM-Informer fusion model and innovatively constructs an attention-enhanced multi-dimensional alarm feature fusion strategy. This

strategy combines the unique equipment types and diagnosis and treatment business scenarios of the hospital network to build a feature system, and uses dynamic weight allocation to solve the problem of multi-source data heterogeneity. This study also designs a Bidirectional LSTM (BiLSTM)-Improved Informer hybrid coding structure (BiLSTM-Informer), introduces a temporal feature enhancement module and an adaptive sparse attention mechanism, and simultaneously improves the ability to capture long-term dependencies and identify short-term sudden threats. The improved Informer in this study is fundamentally different from existing ProbSparse attention-based methods in three core aspects. First, traditional ProbSparse attention selects sparse queries only according to the KL divergence between query vectors and uniform distribution. While the proposed method introduces hospital threat-level prior weights to guide the selection of sparse queries, so that the model pays more attention to alarms from critical medical systems such as DICOM servers and medical device gateways. Second, the sparsity measurement is redefined by combining the threat priority and temporal importance of hospital alarm sequences, which enhances the sensitivity to real threat-related queries and suppresses the interference of redundant alarms. Third, a self-attention distillation mechanism is added to refine long-term features and reduce computational redundancy, enabling the model to capture long-range attack chain correlations more accurately while maintaining high efficiency. Therefore, the improved Informer is no longer a general time-series optimization, but a domain-adaptive sparse attention design for hospital network security scenarios.

The core technical novelties of this study are summarized as follows:

- Hospital domain-adaptive feature fusion: An attention-enhanced heterogeneous feature fusion mechanism is proposed to integrate medical-specific logs (e.g., DICOM servers, medical device gateways) and multi-source alarm data.
- Improved sparse attention with threat priors: Different from standard ProbSparse attention, the proposed Informer introduces threat-level prior weights to guide sparse query selection, improving sensitivity to real threats.
- BiLSTM-Informer hybrid structure: The model simultaneously captures short-term burst features and long-term attack chain dependencies, which cannot be achieved by single LSTM or Informer.
- Lightweight and real-time performance: The optimized model maintains high accuracy while achieving low inference latency, making it suitable for real-time hospital network security systems.

3 Methods

This paper is divided into multi-dimensional alarm feature fusion module and BiLSTM-Informer hybrid coding module. First, it focuses on feature reconstruction and fusion of multi-source alarm data to solve the problem of data heterogeneity. Second, a hybrid coding structure is designed based on fusion features, and accurate research and judgment of hospital NSA are achieved through temporal feature enhancement and attention optimization.

3.1 Multi-Dimensional Hospital Network Alarm Feature Fusion Mechanism Based on Attention Enhancement

Hospital NSA data comes from multiple types of equipment such as firewalls and terminal security equipment, and covers multi-dimensional information such as traffic characteristics, log attributes, and threat intelligence labels. There are significant differences in the dimensions and importance of data of different dimensions. The hospital NSA data source is shown in Figure 1.

In Figure 1, hospital NSA data come from a variety of technical components and operational links, aiming to comprehensively monitor and respond to potential threats. For feature extraction of hospital NSA data, traditional

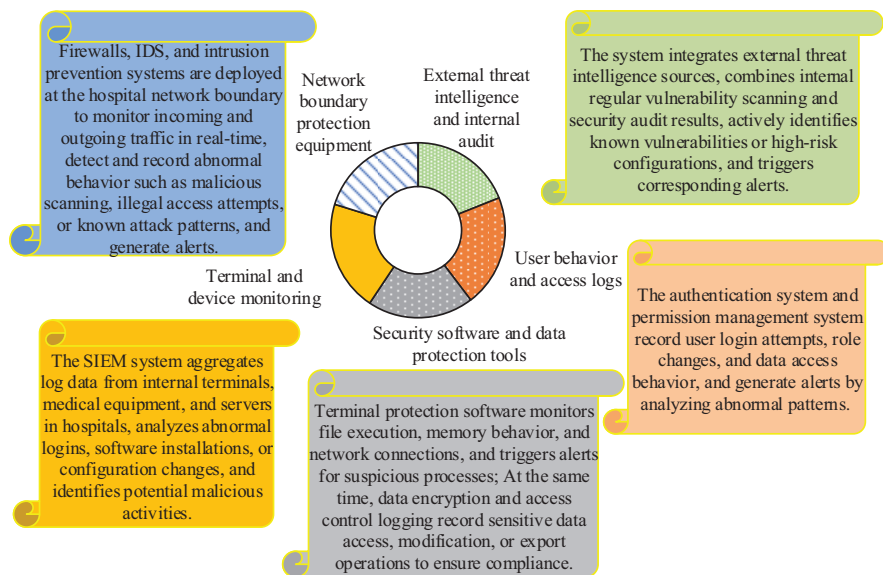


Figure 1 Source of hospital NSA data.

feature fusion uses simple splicing or equal weighting, which cannot distinguish feature importance, resulting in key threat features being diluted by redundant information. Therefore, this study introduces the attention mechanism to construct a feature fusion strategy for dynamic weight allocation, achieves accurate reconstruction of multi-dimensional alarm features, and provides effective input for subsequent hybrid coding modules [13, 14].

First, multi-dimensional alarm feature standardization is carried out. Given the differences in alarm feature dimensions from different equipment sources, an improved Z-score standardization method is adopted. Combined with the time series distribution characteristics of hospital alarm data, the sliding window mean and variance optimization standardization effects are introduced, as shown in Equation (1).

$$X_{i,j}^{norm} = \frac{X_{i,j} - \mu_{j,t}}{\sigma_{j,t} + \epsilon} \quad (1)$$

where $X_{i,j}$ is the j -th dimension original feature of alarm i , $\mu_{j,t}$ is the sliding mean of the j -th dimension feature within the time window t , $\sigma_{j,t}$ is the corresponding sliding variance, $\epsilon = 10^{-6}$ is used to avoid the denominator being 0.

Then, the feature dimension attention weight calculation is performed. An attention scoring function is constructed based on Multi Layer Perceptron (MLP), and the importance weight of each feature dimension is calculated, as shown in Equation (2).

$$\begin{cases} a_j = \text{softmax}(\text{MLP}(W_j \cdot X_{:,j}^{norm} + b_j)) \\ W_j = \text{ReLU}(W_j^1 \cdot W_j^2 + b_j^1) \end{cases} \quad (2)$$

where a_j is the attention weight of the j -th dimension feature, which satisfies $\sum_{j=1}^d a_j = 1$ (d is the total dimension of the feature), W_j and b_j are attention layer parameters, W_j^1 and W_j^2 are MLP hidden layer weight matrices. The ReLU activation function is used to enhance nonlinear feature extraction capabilities [15].

After that, multi-dimensional feature dynamic fusion is performed. Combining the attention weight and standardized features, the final fusion feature vector is generated through weighted summation, as shown in Equation (3).

$$\begin{cases} F_i = \sum_{j=1}^d a_j \cdot X_{i,j}^{norm} + \text{Res}(X_{i,:}^{norm}) \\ \text{Res}(X_{i,:}^{norm}) = X_{i,:}^{norm} - \text{Conv1d}(X_{i,:}^{norm}) \end{cases} \quad (3)$$

where F_i is the fusion feature vector of alarm i , $\text{Res}(\cdot)$ is the residual connection term, which extracts local features through 1-dimensional convolution (Conv1d) and differs from the original features to compensate for the loss of feature information during the attention weighting process [16, 17]. Based on the above, this study first eliminates dimensional differences through standardization, then allocates dynamic weights through the attention mechanism, and finally combines residual connections to optimize feature expression to provide high-quality input for subsequent model encoding.

The generated fusion feature vector $F = [F_1, F_2, \dots, F_N]$ (N is the number of alarm samples) will be used as the input data of the hybrid coding module. Based on the above, the proposed attention-enhanced multi-dimensional alarm feature fusion mechanism is shown in Figure 2.

In Figure 2, fusion features have achieved precise integration and redundant filtering of multi-dimensional information, which can significantly reduce the computational complexity of subsequent encoding modules. At the same time, the fusion features retain the temporal correlation of alarms and key threat characteristics, providing effective support for BiLSTM to capture short-term burst characteristics and improve Informer to analyze long-term dependencies.

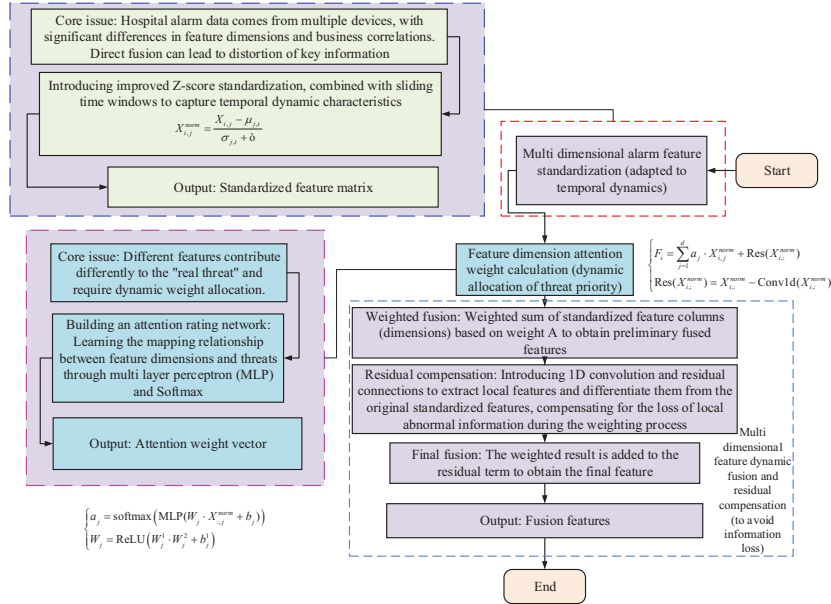


Figure 2 Multi-dimensional alarm feature fusion mechanism with enhanced attention.

3.2 Improved BiLSTM-Informer

Hospital NSA data have two key characteristics: short-term burstiness and long-term continuity [18]. A single LSTM model has a gradient decay problem in long time sequence analysis, and it is difficult to capture long-term attack chain correlations. Although the basic Informer optimizes long sequence processing efficiency through sparse attention, its response sensitivity to short-term burst features is insufficient. Therefore, this study designs the BiLSTM-Informer structure based on the obtained fusion features. It extracts short-term bidirectional temporal features through BiLSTM, captures long-term dependencies by improving the adaptive sparse attention mechanism of Informer, and then achieves complementary enhancement of the two types of features through the feature fusion layer, and finally outputs alarm research and judgment results (real threats/false alarms). First, BiLSTM is used to extract short-term temporal features. BiLSTM is shown in Figure 3.

In Figure 3, based on the fused feature sequence $F = [F_1, F_2, \dots, F_T]$ (T is the timing window length), a BiLSTM network is constructed to extract short-term timing dependencies from the forward and reverse directions. It captures the before and after dependencies of short-term alarm sequences through bidirectional scanning and improves the sensitivity of identifying sudden alarms. The forward extraction formula is shown in Equation (4).

$$\vec{h}_t = \text{LSTM}_{\vec{W}}(F_t, \vec{h}_{t-1}) = o_t \odot \tanh(c_t) \quad (4)$$

where $\vec{h}_t$ is the hidden state of forward LSTM at time step t , and its calculation follows the LSTM gating mechanism. The reverse extraction is shown in

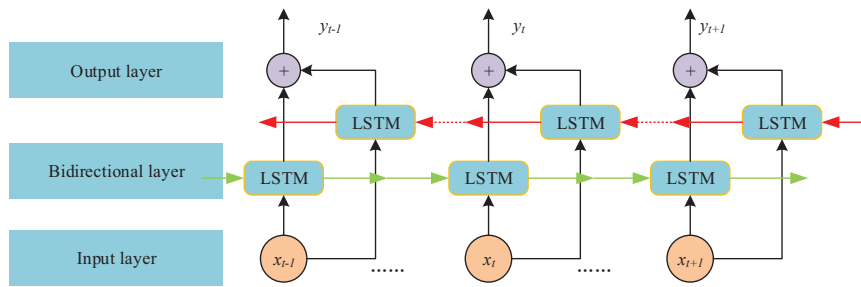


Figure 3 BiLSTM structure.

Equation (5).

$$\overleftarrow{h}_t = \text{LSTM}_{\overleftarrow{W}}(F_t, \overleftarrow{h}_{t+1}) \quad (5)$$

where $\overleftarrow{h}_t$ is the hidden state of reverse LSTM at time step t , following the LSTM gating mechanism [19, 20]. The short-term temporal feature fusion is shown in Equation (6).

$$h_t^{\text{short}} = \text{Concatenate}(\vec{h}_t, \overleftarrow{h}_t) \cdot W_s + b_s \quad (6)$$

where h_t^{short} is the short-term time series feature after fusion. The bidirectional hidden state is spliced through the Concatenate function, and then the feature dimension is optimized through linear transformation (W_s and b_s are transformation parameters). This research design improves the adaptive sparse attention mechanism of Informer, as shown in Figure 4.

In Figure 4, to address the problem of insufficient adaptability of the basic Informer's ProbSparse attention mechanism to hospital alarm data, a priori information on alarm threat levels is introduced to optimize sparse query selection. Among them, the Kullback-Leibler Divergence (KL) (sparse query

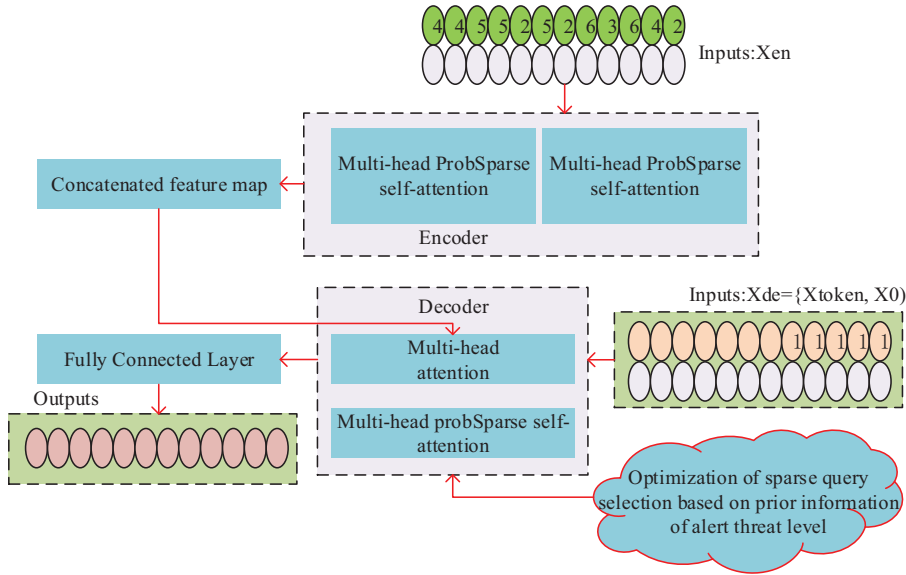


Figure 4 Improved Informer model.

sparsity measure) is calculated as shown in Equation (7).

$$KL(q_i \| p) = \sum_{k=1}^L q_i(k) \log \frac{q_i(k)}{p(k)} \quad (7)$$

where $KL(q_i \| p)$ is the KL divergence between the i -th query vector q_i and the uniform distribution p , which is used to measure sparsity. The query vector distribution introducing threat level prior is shown in Equation (8).

$$q_i(k) = \frac{\exp(q_i \cdot k^T / \sqrt{d_k})}{\sum_{k'=1}^L \exp(q_i \cdot k'^T / \sqrt{d_{k'}})} \cdot \alpha \cdot l_i \quad (8)$$

where l_i is the prior weight of the alarm threat level (core business system alarm $l_i = 1.2$, ordinary alarm $l_i = 0.8$), and $\alpha = 0.1$ is the weight adjustment coefficient. The sparse query matrix selection is shown in Equation (9).

$$Q' = \text{Top} - \text{U}(Q, \text{score}(q_i) = KL(q_i \| p)) \quad (9)$$

where Q' is a sparse query matrix composed of selecting Top-U query vectors with high sparsity scores. The adaptive sparse attention calculation is shown in Equation (10).

$$\text{Attn}(Q', K, V) = \text{softmax} \left(\frac{Q' K^T}{\sqrt{d_k}} \right) V \quad (10)$$

where $\text{Attn}(\cdot)$ is the final adaptive sparse attention calculation result.

After that, long-term feature extraction and fusion are performed, and the adaptive sparse attention output is refined through the self-attention distillation layer, and then fused with the short-term features extracted by BiLSTM. Long-term feature distillation is shown in Equation (11).

$$\begin{aligned} h_t^{long} &= \text{Distill}(\text{Attn}(Q', K, V)) \\ &= \text{MaxPool}(\text{ELU}(\text{Conv1d}(\text{Attn}(Q', K, V)))) \end{aligned} \quad (11)$$

where $\text{Distill}(\cdot)$ is the self-attention distillation operation, which implements feature refinement and reduces redundant information through 1D convolution, exponential linear unit activation, and maximum pooling. h_t^{long} is a long time series feature. The dynamic fusion of long and short time series features is shown in Equation (12).

$$h_t^{fusion} = \beta \cdot h_t^{short} + (1 - \beta) \cdot h_t^{long} \quad (12)$$

where h_t^{fusion} is the long and short time series fusion feature. The calculation of dynamic fusion weight is shown in Equation (13).

$$\beta = \text{sigmoid}(\text{MLP}(h_t^{short} \oplus h_t^{long})) \quad (13)$$

where β is the dynamic fusion weight, and the importance ratio of the two types of features is learned through MLP. $\oplus$ is the feature splicing operation.

3.3 Hospital NSA Model

This study applies the output of the model to hospital NSA. Specifically, the fusion features are input into the fully connected layer and the sigmoid activation function, and the probability that the alarm is a real threat is output, as shown in Equation (14).

$$P(y_t = 1|F_{1:T}) = \text{sigmoid}(W_o \cdot h_t^{fusion} + b_o) \quad (14)$$

where $y_t = 1$ is the alarm t , which is a real threat, and $y_t = 0$ is a false alarm. W_o and b_o are output layer parameters. In addition, considering the low proportion of real threat samples in hospital alarm data (positive samples are scarce), Focal Loss is used as the training objective function to alleviate the impact of category imbalance, as shown in Equation (15).

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^N (1 - P_i)^\gamma \cdot y_i \log(P_i) + P_i^\gamma \cdot (1 - y_i) \log(1 - P_i) \quad (15)$$

where P_i is the predicted probability of the i -th sample, $\gamma = 2$ is the focus parameter, which improves the model's learning ability for difficult-to-classify samples (real threats) by reducing the weight of easy-to-classify samples (false positives) [21, 22]. Through the above, this research has formed a complete hybrid coding research and judgment logic. First, short-term features are extracted through BiLSTM, and then long-term features are obtained through improved Informer. Finally, accurate alarm analysis and judgment is achieved through dynamic fusion and output layer, as shown in Figure 5.

In Figure 5, the constructed hybrid coding research and judgment logic takes multi-dimensional fusion features as input, captures the temporal dependencies of short-term sudden alarms through BiLSTM, and uses the improved Informer that introduces hospital threat priors to mine long-term attack chain correlations. After the gating mechanism dynamically fuses

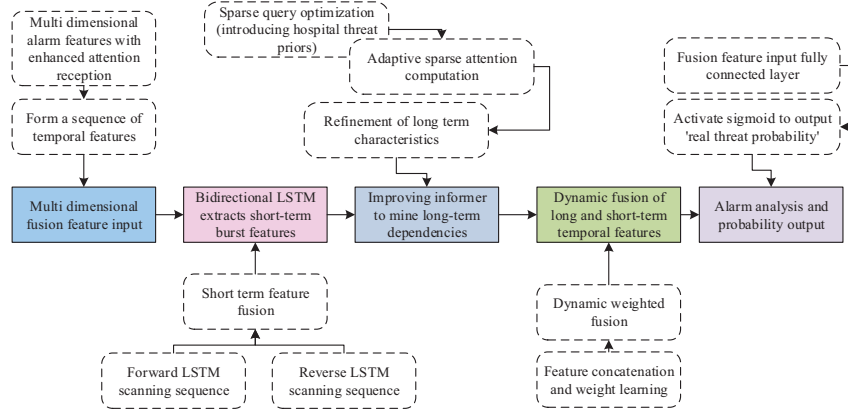


Figure 5 The proposed mixed coding analysis process.

the two types of features, and the fully connected layer is combined with Focal Loss training, the real threat probability is output, achieving collaborative research and judgment of “accurate identification of short-term alarms + complete characterization of long-term attacks”.

4 Results

An experiment is carried out to verify the research method, corresponding design parameters and experimental data results are analyzed, and the advantages and feasibility of the method are verified.

4.1 Experimental Data and Settings

The experimental data came from the NSA data of a certain hospital, covering alarm records of six devices including firewall, WAF, and terminal security (one month), with a total of 136,022 samples. The data preprocessing process included deleting invalid missing samples (accounting for 2.3%), labeling real threat/false positive labels (based on the judgment of security experts, real threat samples account for 4.7%), and dividing the training set and the test set at a ratio of 7:3. The dataset covered nine typical attack types and normal network behaviors, with detailed distribution as follows: normal behaviors account for 95.3% (129,626 samples). It included regular medical service access (DICOM image transmission, electronic medical record query) and office network traffic. Real threat samples accounted for

4.7% (6396 samples), among which port scanning accounts for 1.2% (1632 samples), intranet lateral movement accounted for 0.8% (1088 samples), encrypted malicious payload propagation accounted for 0.7% (952 samples), malicious traffic injection accounted for 0.6% (816 samples), data leakage attempts accounted for 0.5% (680 samples), malicious macro script execution accounted for 0.4% (544 samples), unauthorized DICOM configuration modification accounted for 0.3% (408 samples), weak password brute-force attack accounted for 0.15% (204 samples), and unauthorized cloud storage synchronization accounted for 0.05% (68 samples). The hospital alarm dataset had a serious category imbalance problem (the proportion of real threat samples is only 4.7%), which might lead to the model's overfitting to normal samples and low recognition accuracy of threat samples. To solve this problem, this study adopted a combination of data enhancement and loss function optimization for targeted improvement:

- Data enhancement for minority threat samples: Time series data enhancement methods such as random time warping, noise injection (Gaussian noise with mean 0 and variance 0.01), and sample interpolation were used to expand the real threat samples by 3 times (from 6396 to 19188 samples), which effectively increased the diversity of threat feature samples and avoided the model's insufficient learning of minority classes.
- Focal Loss as the training objective function: As shown in Equation (15), Focal Loss reduced the weight of easy-to-classify normal samples by setting the focus parameter $\gamma = 2$, and increased the learning weight of difficult-to-classify threat samples, which further alleviated the impact of category imbalance on model performance and improves the model's ability to identify real threats in unbalanced data.

To verify that the proposed model had no overfitting and had good generalization ability on different network security datasets, this study additionally conducted a cross-dataset verification experiment using the CICIDS2017 dataset – a classic public SOTA dataset in the field of network intrusion detection, which was widely used in existing network threat detection research and included multiple typical attack types (DDoS, port scanning, brute force attack) with balanced and unbalanced sample subsets. The CICIDS2017 dataset was preprocessed in the same way as the hospital actual dataset (deleting invalid samples, standardizing features, dividing training and test sets at 7:3), and the proposed model and comparison models were trained with the same parameters to ensure the fairness of verification.

Table 1 Model parameter settings

Category	Name	Parameter	Category	Parameter	Value
Feature fusion layer	MLP hidden layer dimension	128	Optimizer	Optimizer type	AdamW
BiLSTM module	Number of layers	2		Initial learning rate	0.0001
	Hidden layer dimension	256		Learning rate adjustment strategy	Cosine annealing
	Time window length (T)	60	Training configuration	Training batch size	256
Improved Informer module	Number of encoder stacks	3		Iteration count	100
	Number of attention heads	8		Early stop patience value	10
	Top-U selection ratio	0.2	/	/	/

The data were collected from six core devices: firewall (35% of total samples), WAF (25%), terminal security software (18%), medical device access gateway (12%), DICOM server audit logs (6%), and cloud storage security gateway (4%). All threat labels were jointly confirmed by three senior network security engineers with more than 5 years of hospital network security experience, and the inter-annotator agreement (IAA) reached 0.94, ensuring label reliability. The model configuration is shown in Table 1.

The experiment is carried out from two dimensions – model performance evaluation and ablation experimental verification – and the superiority of the optimized LSTM-Informer model was verified through comparison. The experiment used Accuracy, Precision, Recall, F1 score, and FAR as core evaluation indicators. All experiments were implemented based on the PyTorch framework, and the hardware environment was Intel Xeon Gold 6230 processor and RTX4090 graphics card. Four types of mainstream timing analysis models were used for comparison: (1) traditional LSTM model. (2) basic Informer model. (3) LSTM-Convolutional Neural Network (CNN) model (the mainstream hybrid model of existing NSA analysis). (4) Gated Recurrent Unit (GRU) model (a simplified version of the gated recurrent network, used to compare the effects of the gating mechanism). All comparison models were trained based on the same preprocessed data and experimental parameters to ensure fairness in comparison.

To further verify the superiority of the proposed model compared with SOTA methods, two representative SOTA models that were highly relevant to

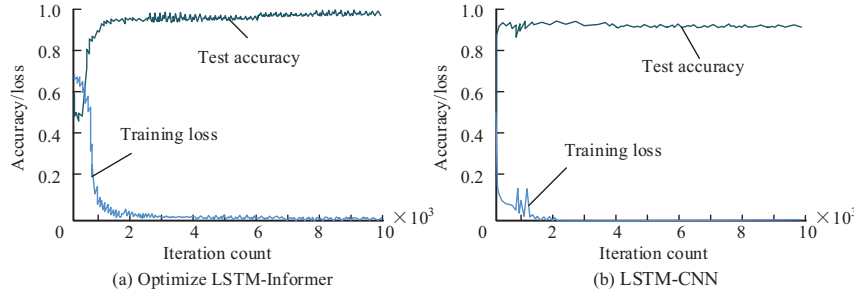


Figure 6 Training loss and testing accuracy of various alarm models.

the research task of hospital network threat detection (time series classification + network security log anomaly detection) were selected for comparison. The selection basis and model characteristics were as follows:

- Temporal Fusion Transformer (TFT) [23]: a classic SOTA model for time series classification with multi-head attention and gating mechanisms, which was widely used in time series anomaly detection tasks and had strong ability to capture global temporal feature fusion, making it a typical comparison model for time series-based network threat detection.
- DeepLog [24]: a SOTA method specifically designed for network security log anomaly detection, which was the most representative model in log-based intrusion detection and was widely cited in existing NSA research, making it a typical comparison model for log-based hospital network threat detection.

4.2 Model Performance Analysis

Figure 6 shows the training loss and test accuracy of the research model and existing models. The comparison model was LSTM-CNN. In Figure 6(a), as the number of iterations increases, the accuracy of the research model improved significantly after approximately 0.24×10^3 iterations. As the loss value decreased, the accuracy continued to increase and eventually stabilized. The loss value gradually approached 0, which indicated that the model had good convergence. In Figure 6(b), the accuracy of LSTM-CNN remained stable after iterations reached about 2.11×10^3 times, and the accuracy decreased when iterations reached about 4.38×10^3 times.

Table 2 is a comparison of the performance indicators of each model on the test set. The optimized LSTM-Informer model performed best in all

Table 2 Comparison of performance indicators of various models on the test set

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)	FAR (%)
LSTM	89.6	88.2	85.3	86.7	10.8
Basic Informer	91.1	90.5	87.8	89.1	9.2
LSTM-CNN	90.3	89.7	86.5	88.1	11.7
GRU	88.9	87.5	84.1	85.8	12.3
Optimized LSTM-Informer	95.3	94.8	92.6	93.7	3.2

indicators: the accuracy reached 95.3%, which was 4.2% higher than the basic Informer and 5.7% higher than the traditional LSTM. The recall rate reached 92.6%, which was significantly better than other models, indicating that the model had a stronger ability to identify real threats. FAR was as low as 3.2%, which was 8.5% lower than LSTM-CNN, effectively alleviating the problem of alarm fatigue.

To further intuitively demonstrate the model performance, the Receiver Operating Characteristic (ROC) curve and PR (Precision-Recall) curve of each model were drawn, as shown in Figure 7. In Figure 7(a), the PR curve of the optimized LSTM-Informer model was always above the comparison model (LSTM, Basic Informer, LSTM-CNN, GRU). In the core range of recall rate 0.6~0.8, its precision was 8~12% higher than the basic Informer. This showed that while ensuring the real threat detection rate (recall), the model could filter false positives more efficiently (improving precision) and adapted to the hospital's security operation needs of "fewer false negatives and lower false positives". In Figure 7(b), the ROC curve of the optimized LSTM-Informer was closer to the upper left corner of the coordinates: When the False Positive rate (FP Indicator) was <0.2 , its True Positive rate (TP Indicator) had exceeded 0.85, which was about 15% higher than LSTM. The rising section of the curve was steeper, indicating that the model could still efficiently identify real threats under low false alarm thresholds, verifying the fusion structural advantages of "BiLSTM capturing short-term burst features + improved Informer mining long-term dependencies".

As shown in Table 3, the proposed model outperformed the SOTA methods in all core indicators. Compared with TFT, the accuracy was improved by 1.5%, recall by 2.5%, and FAR was reduced by 2.5 percentage points. Compared with DeepLog, the accuracy was improved by 1.2%, recall by 2.9%, and FAR was reduced by 3 percentage points. The key advantage lay in the hybrid coding structure: TFT focused on global temporal feature

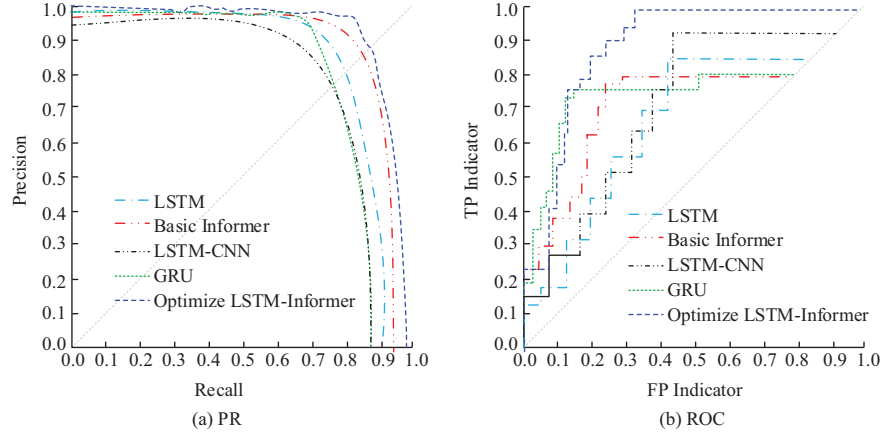


Figure 7 ROC and PR curves of each model.

Table 3 Performance comparison with SOTA methods

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)	FAR (%)
TFT	93.8	92.6	90.1	91.3	5.7
DeepLog	94.1	93.2	89.7	91.4	6.2
Optimized LSTM-Informer (Proposed)	95.3	94.8	92.6	93.7	3.2

fusion but lacked adaptability to hospital-specific threat patterns. DeepLog excelled in log sequence anomaly detection but had insufficient sensitivity to short-term burst alarms. In contrast, the proposed model's attention-enhanced multi-dimensional feature fusion module effectively integrated hospital-specific data (e.g., DICOM protocol features, medical device logs), and the BiLSTM-Informer hybrid structure balanced long-term attack chain mining and short-term threat capture, thus achieving better performance in hospital NSA research and judgment.

The ablation results (Table 4) demonstrate that each proposed module effectively enhanced detection performance. The standalone Basic Informer and BiLSTM models yielded relatively low accuracy and recall, along with high FARs. Integrating the attention mechanism significantly boosted accuracy and recall while reducing false alarms. By combining BiLSTM, improved Informer, and attention, the proposed model achieved the highest accuracy of 95.3%, recall of 92.6%, and the lowest FAR of 3.2%, validating the rationality and effectiveness of the full hybrid framework.

Table 4 Ablation study of key modules

Model Setting	Accuracy (%)	Recall (%)	FAR (%)
Basic Informer	91.1	87.8	9.2
BiLSTM alone	90.7	86.9	8.7
Informer + Attention	93.4	90.5	5.6
BiLSTM + Attention	92.8	89.8	6.1
Proposed (BiLSTM + Improved Informer + Attention)	95.3	92.6	3.2

Although the proposed optimized LSTM-Informer model showed a moderate numerical improvement over the SOTA models (TFT and DeepLog) on the core evaluation indicators, it had irreplaceable scenario adaptability and comprehensive performance advantages for hospital network threat detection compared with the general SOTA models. The marginal improvement in indicators was of great practical significance for hospital network security (even a 1% improvement in recall rate could reduce the missed detection of critical medical network threats). The specific advantages were better performance on unbalanced data and cross-dataset generalization ability. The proposed model adopted data enhancement and Focal Loss to solve the category imbalance problem of hospital alarm data, and the cross-dataset verification on the classic SOTA dataset CICIDS2017 showed that the model had good generalization ability (the accuracy, recall, and F1 score on CICIDS2017 are 94.8%, 91.9%, and 93.3%). In contrast, TFT and DeepLog showed significant performance degradation on unbalanced hospital alarm data (the recall rate was reduced by more than 5%) and had poor generalization ability on cross-datasets, which was difficult to apply to the actual hospital network environment with serious data imbalance.

4.3 Hospital NSA Model Application Analysis

Figure 8 shows the comparison and error distribution between the actual alarm results and the research model output. Figure 8(a) presents the comparison between the actual alarm results and the output of the research model. The orange model outputted column and the blue actual result column were highly coincident in most tests (such as test 1, 9, 25 and other typical nodes), reflecting the consistency between the optimized LSTM-Informer's recognition results of real threats and the judgment of security experts, verifying the high accuracy of the model. Figure 8(b) shows the error distribution through a biaxial polyline. The relative error and absolute error were maintained at a

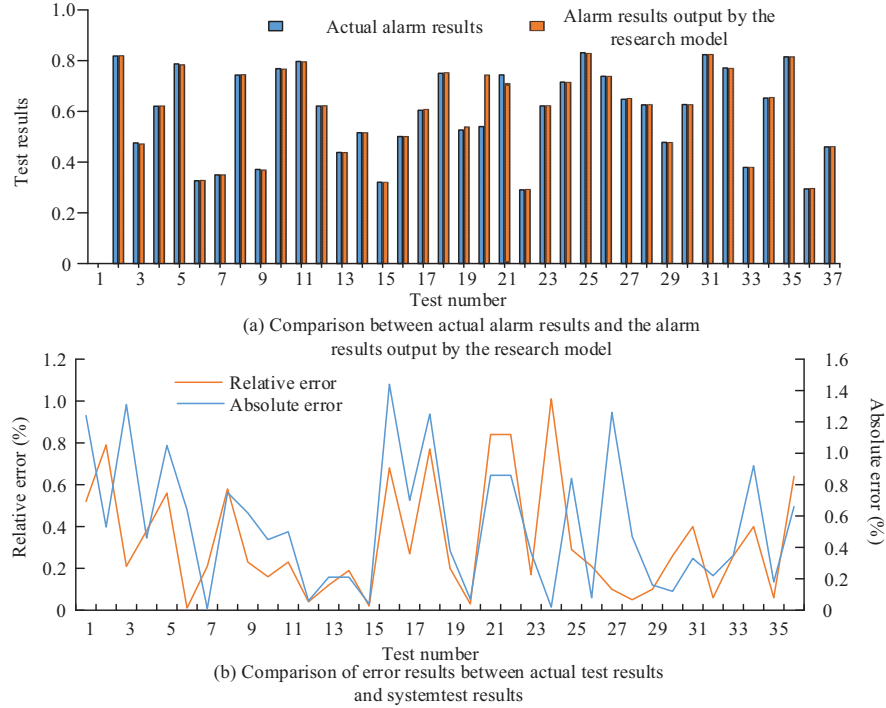


Figure 8 Error distribution between actual alarm results and research model output.

low level of less than 1%. Although there were local fluctuations at test nodes such as 17 and 23 due to the increase in the complexity of the alarm features, the overall trend was stable. This reflected the model's prediction stability under multiple types of alarm samples and provided reliable support for the core requirement of "reducing false alarms and identifying real threats" in hospital network security operations.

Figure 9 shows the comparison of alarm times for malicious behaviors, normal behaviors, and credit behaviors of different hospital NSA models. In Figure 9(a), the optimization-based LSTM-Informer significantly differentiated the timing characteristics of malicious behavior, normal behavior, and credit behavior. The alarm time peaks of malicious behaviors near time window numbers 10–20 and 30 were sharper, and there was less overlap with the curves of normal/credit behaviors (separation degree $>30\%$), which reflected the model's accurate capture of attack timing patterns. In Figure 9(b), the three types of behavior curves of LSTM-CNN were intertwined (such as the time window number 20–30 interval, the coincidence degree

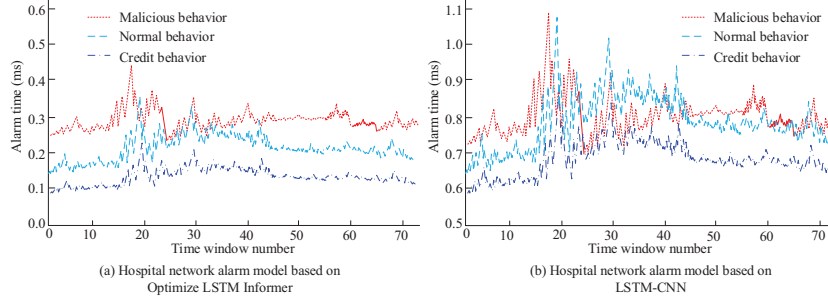


Figure 9 Alarm time for malicious, normal, and credit behaviors in different hospital NSA models.

of malicious and normal behavior curves exceeded 60%). The peak value of malicious behavior was “submerged” in normal fluctuations, reflecting its insufficient ability to distinguish complex temporal features. This difference stemmed from the synergy mechanism of the optimization model, while the convolutional sliding window of LSTM-CNN had limited ability to depict long-term correlations, resulting in distortion of temporal pattern recognition of malicious behaviors.

The performance of the optimized LSTM-Informer under different hospital NSA types is shown in Table 5. Among the long-series correlation alarm types, the recall rate of port scanning, intranet lateral movement, and encrypted malicious payload propagation were all $\geq 94.5\%$, and the FAR was $\leq 2.8\%$, which proved that the model effectively filtered redundant alarms in long-series. Among the short-term burst alarm types, the F1 score of malicious traffic injection and data leakage attempts was $\geq 93.8\%$. Since the characteristics of malicious macro script execution were more subtle, the FAR was slightly higher (4.0%), but it was still far lower than traditional LSTM (10.8%). Among the protocol-specific alarm types, unauthorized DICOM configuration modification was due to complex protocol fields and blurred normal/abnormal boundaries. Although the model accuracy rate (92.8%) was lower than other types, it still reached more than 90%, which verified the adaptability of the feature fusion module to heterogeneous protocols.

To verify the practical deployability in hospital environments, inference time and model scale were tested. The proposed model processed one alarm sample within 1.8 ms, and the average latency for a batch of 256 samples was 14.3 ms, fully meeting the real-time requirements (≤ 50 ms) of hospital network monitoring systems. The parameter scale of the model was 3.78 MB, which was lightweight enough to run on edge security devices or

Table 5 Performance of optimized LSTM-Informer under different types of hospital NSA

		Accuracy	Precision	Recall	F1 score	FAR
Alarm Type		(%)	(%)	(%)	(%)	(%)
Long-term correlation type	Port scan alarm (continuous detection)	96.2	95.8	94.5	95.1	2.8
	Horizontal internal network movement (attack chain)	95.8	95.3	94.7	95	2.6
	Encrypted malicious payload propagation	96.5	96	95.2	95.6	2.3
Short term sudden onset	Malicious traffic injection (instantaneous attack)	94.8	94.2	93.5	93.8	3.5
	Data leakage attempt (file transfer)	95.5	95	94	94.5	2.5
	Malicious macro script execution	94.2	93.5	92.8	93.1	4
Protocol special type	Unauthorized DICOM configuration modification	92.8	91.5	90.7	91.1	5.1
High frequency repetitive type	Weak password login attempt (brute force cracking)	93.5	92.7	91.2	91.9	4.2
Boundary breakthrough type	Unauthorized cloud storage synchronization	93.9	93.2	92.5	92.8	4.3

standard hospital servers. Compared with traditional deep learning models, the proposed method maintained high detection accuracy while achieving low computational overhead, enabling real-time threat detection without affecting the stability of medical business systems.

Real-time performance and computational cost were evaluated for hospital deployment. The average inference latency was 1.8 ms per sample and 14.3 ms for a batch of 256 samples, which fully satisfied the real-time requirement of hospital network monitoring. The model size was only 3.78 MB, enabling lightweight deployment on edge security devices. The computational complexity was 1.26 GFLOPs per sample with stable CPU usage, indicating that the model met the efficiency constraints of practical hospital network environments.

5 Discussion and Conclusion

This study proposed a hospital NSA model based on optimized LSTM-Informer, which achieved accurate research and judgment of massive alarms

through attention-enhanced multi-dimensional feature fusion and BiLSTM-Informer hybrid structure. The recall rate of long sequence related alarm types was $\geq 94.5\%$, $FAR \leq 2.8\%$. In short-term sudden alarm types, the F1 score for malicious traffic injection and data leakage attempts was $\geq 93.8\%$. Since the characteristics of phishing emails were more subtle, the FAR was slightly higher (4.0%), but it was still far lower than the traditional LSTM model (10.8%). The proposed hybrid model that integrated long-term and short-term time series characteristics was more suitable for the dual characteristics of hospital network alarm data. The optimization strategy that introduced domain prior information could further improve the scene adaptability of the model. However, this paper also has certain limitations. Model training relied on a large number of labeled samples, and the ability to identify new unknown threats needed to be improved, not considering the lightweight deployment requirements for edge devices. Future work can introduce a federated learning framework to achieve joint training of multi-hospital alarm data to improve model generalization capabilities. It can also explore model lightweight optimization strategies to adapt to the deployment needs of edge security devices. In addition, it can be combined with generative AI technology to simulate attack scenarios and enhance the ability to identify unknown threats.

References

- [1] Zhou X, Li B. Cybersecurity Situational Awareness Model using Improved LSTM-Informer. *International Journal of Computer Science and Information Technology*, 2024, 2(3):37-49. DOI:10.62051/ijcsit.v2n3.05.
- [2] Singha A K, Singh H P, Kundu S, Tiwari P K, Rajput A S. Estimating Computer Network Security Scenarios with Association Rules. *Journal of Discrete Mathematical Sciences and Cryptography*, 2024, 27(2–A):223-236. DOI:10.47974/jdmsc-1876.
- [3] Jevák J, Kelemen M, Rozenberg R, L'Ubomír T. Innovative Software Tool for Cyber Security against Security Incidents in Civil Aviation Network Operations. *New Trends in Aviation Development (NTAD)*, 2024, 1(1):73–78. DOI:10.1109/ntad63796.2024.10850485.
- [4] Liu G, Zhang Y, Zhang M. Analysis of the Current State of Network Security Alert Management and Recommendations. *Fifth International Conference on Computer Communication and Network Security (CCNS 2024)*, 2024, 1(1):52–53. DOI:10.1117/12.3038182.

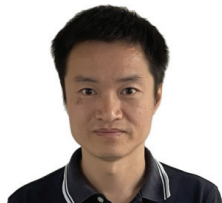
- [5] Shankar A, Madiseti V. A Framework for Cybersecurity Alert Distribution and Response Network (ADRIAN). *Journal of Software Engineering and Applications*, 2024, 17(5):396–420. DOI:10.4236/jsea.2024.175022.
- [6] Kalakoti R, Vaarandi R, Bahi H, Nomm S. Evaluating Explainable AI for Deep Learning-Based Network Intrusion Detection System Alert Classification. *Proceedings of the 11th International Conference on Information Systems Security and Privacy*, 2025, 1(1):47–58. DOI:10.5220/0013180700003899.
- [7] Jalalvand F, Chhetri M B, Nepal S, Paris C. Alert Prioritisation in Security Operations Centres: A Systematic Survey on Criteria and Methods. *ACM Computing Surveys*, 2025, 57(2):1–36. DOI:10.1145/3695462.
- [8] Huang L, Ye W, He J. Network Security Threat Prevention and Control System for Wind Farm Power Monitoring System. 2024 International Conference on Power, Electrical Engineering, Electronics and Control (PEEEEC), 2024, 1(1):290–295. DOI:10.1109/peeec63877.2024.00059.
- [9] Zuberi A H, Ahmad S. IoT Based Smart Alert Network Security System Using Machine Learning. *International Journal of Innovative Research in Computer Science and Technology*, 2023, 11(4):15–23. DOI:10.55524/ijrcst.2023.11.4.4.
- [10] Vaarandi R, Guerra-Manzanares A. Network IDS Alert Classification with Active Learning Techniques. *Journal of Information Security and Applications*, 2024, 81(1):103687. DOI:10.1016/j.jisa.2023.103687.
- [11] Huang X, Chen N, Deng Z, Huang S. Multivariate Time Series Anomaly Detection via Dynamic Graph Attention Network and Informer. *Applied Intelligence*, 2024, 54(17–18):7636–7658. DOI:10.1007/S10489-024-05575-Y.
- [12] Elezmazy I M, Mostafa N N. Enhanced Network Security using LSTM-Based Autoencoder Models. *Artificial Intelligence in Cybersecurity*, 2024, 1(1):60–69. DOI:10.61356/j.aics.2024.1315.
- [13] Momposhi L, Maurushat A, Calheiros R N, Khan S. Next-Gen Threat Hunting: A Comparative Study of ML Models in Android Ransomware Detection. *FinTech and Sustainable Innovation*, 2025, 1(1):A3–A4. DOI:10.47852/bonviewFSI52025685.
- [14] Cui W, Liao X, Yang Y, Feng S, Song M. Informer-based DDoS Attack Detection Method for the Power Internet of Things. *PLOS One*, 2025, 20(5):e0322329.1–e0322329.2. DOI:10.1371/journal.pone.0322329.
- [15] Dharshiniya S, Daniel M R S. IoT Network Intrusion Detection with Deep Learning and Voice Alerts. 2024 International Conference on

- IoT Based Control Networks and Intelligent Systems (ICICNIS), 2024, 1(1):354–360. DOI:10.1109/icicnis64247.2024.10823385.
- [16] Xiao L, Pan T H, Wu X, Zhu Y K. Research on Security Situation Assessment and Prediction Model of Network System in Deep Learning Environment. *Journal of Cyber Security and Mobility*, 2024, 13(6):1263–1282. DOI:10.13052/jcsm2245-1439.1362.
- [17] Chen Z. Campus Network Security Intrusion Detection Based on Feature Segmentation and Deep Learning. *Journal of Cyber Security and Mobility*, 2024, 13(4):775–802. DOI:10.13052/jcsm2245-1439.1349.
- [18] Wu Q. Network Security Maintenance and Detection Based on Diversified Features and Knowledge Graph. *Journal of Cyber Security & Mobility*, 2025, 14(2):339–364. DOI:10.13052/jcsm2245-1439.1424.
- [19] Zhang H, Meng F, Wang Q. Computer Network Security System Optimization Based on Improved Neural Network Algorithm and Data Search. *Journal of Cyber Security & Mobility*, 2025, 14(1):75–100. DOI:10.13052/jcsm2245-1439.1414.
- [20] Riebe T. CySecAlert: An Alert Generation System for Cyber Security Events Using Open Source Intelligence Data. *Technology Assessment of Dual-Use ICTs*, 2023, 1(1):249–265. DOI:10.1007/978-3-658-41667-6_15.
- [21] Ramirez A G, Sardy L A, Ramirez F G. Tikuna: An Ethereum Blockchain Network Security Monitoring System. *Lecture Notes in Computer Science*, 2023, 1(1):462–476. DOI:10.1007/978-981-99-7032-2_27.
- [22] Sathiyamoorthi A S A, Senthil S R, Vittaldass S, Raman R. Anti-Theft Alert System for Home Security. 2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON), 2024, 1(1):1–5. DOI:10.1109/delcon64804.2024.10867266.
- [23] Song K, Wu Y, Fan J. MTFT: Multimodal Temporal Fusion Transformer for 3D Human Pose and Shape Estimation. *Signal, Image and Video Processing*, 2025, 19(13):1–12. DOI:10.1007/s11760-025-04741-0.
- [24] Aziz A, Munir K. Anomaly Detection in Logs Using Deep Learning. *IEEE Access*, 2024, 12(1):176124–176135. DOI:10.1109/access.2024.3506332.

Biographies



Hanteng Liu obtained his master's degree in Medicine from Sun Yat-sen University, China, in 2004. Currently, he serves as Section Chief of the Statistics, Network Management Section at The First Affiliated Hospital, Sun Yat-sen University, with over 10 years of working experience in hospital informatization. He has presided over the construction and upgrading of the platform-based electronic medical record system, the practical deployment of regional smart medical collaboration, and the development of cybersecurity architecture for smart hospital defense scenarios in the hospital. He has led teams to participate in numerous authoritative national and provincial competitions and achieved outstanding awards, fostering a positive talent development philosophy of promoting learning, training and innovation through competitions, including one national first prize, two national second prizes and three national third prizes. He has also rich academic and practical achievements, including three patents, 10 academic papers, five monographs, eight compiled group standards, three software copyrights, and five professional honors and social part-time positions.



Zonggeng Chen, Engineer, holds a master of engineering degree in Computer Technology from Sun Yat-sen University, China. He currently serves as the Team Leader of the Cybersecurity Group, Network Management Department, Information and Data Center, The First Affiliated Hospital of

Sun Yat-sen University. He is also a Standing Committee Member of the Medical Professional Committee of the Provincial Computer Information Network Security Association (2023–2027) and a Member of the Information Branch of the Provincial Health Economics Association (2024–2027). He has long been dedicated to cybersecurity work in hospital informatization construction, with extensive experience in the management and implementation of hospital cybersecurity projects. In addition, he has organized teams to participate in national and provincial-level “Huwang” (cyber defense) exercises, possessing rich hands-on experience in cybersecurity operations.



Yishun Xia earned his master’s degree in Computer Science and Engineering from University of Glasgow, UK. He is working as staff in Center for Information Technology & Statistics, Network Management Section, The First Affiliated Hospital of Sun Yat-sen University, China. His main research interests lie in network security and traffic log analysis. He achieved excellent results in the National Cybersecurity Defense Competition for the Health Industry. He promoted the tightening of the VPN network boundary for operation and maintenance. By implementing refined access permission control, optimizing access rules, strengthening internal and external network isolation, and deploying virtual machine detection, which greatly improved the defense capability of internal network boundaries.



Siqi Qiao obtained the Master of Science in Advanced Computer Science by the University of York in 2022. Currently, she works at Center for Information Technology & Statistics, The First Affiliated Hospital, Sun Yat-sen University. She has participated in and overseen a series of security initiatives, such as cybersecurity services and data security governance. She has co-authored papers on data classification and grading as well as security governance frameworks, and has conducted research on cybersecurity topics related to large language models in specific domains. She specializes in hospital data security governance, big data applications, and intelligent algorithm development, closely aligning her work with the needs of digital transformation in healthcare and accumulating practical experience in the field.



Jiayu Ou holds a bachelor's degree from South China University of Technology (SCUT) and currently serves as Deputy General Manager at Guangzhou Zhongke Mingnuo Data Co. Ltd. With over 12 years of experience in the cybersecurity industry and more than 10 years in security consulting, he is well-versed in the development of information security specifications for multiple industries in China and has actively contributed to such efforts. His research expertise covers adaptive cyber offense-defense confrontation,

collaborative security protection systems, quantum secure communication, and knowledge graphs for data security. He has applied his expertise to key national research projects including the development of the Cyberspace Security Joint Laboratory for China Southern Power Grid, as well as major provincial projects such as the Key Enterprise Laboratory Project for Power System Cybersecurity of Guangdong Province.