International Journal for Housing Science and Its Applications
Publish August 4, 2025. Volume 46, Issue 3 Pages 2536-2547

https://doi.org/10.70517/ijhsa463212

Construction of Emergency Safety Response System for Energy Industry by Integrating Multimodal Data

Bo Liu[1] and Hongke Li[1,*]
[1] Yunding Technology Co., Ltd., Jinan, Shandong, 250000, China
Corresponding authors: (e-mail: 13361075351@163.com).

Abstract With the digital transformation of industrial enterprises, the energy industry environment faces increasingly complex network security and information security issues. Based on Kubernetes cluster management system, the article establishes an emergency security response system for the energy industry and designs a series of functional modules for data collection, security detection and emergency response. In order to improve the network intrusion detection capability of the emergency security response system, this paper proposes a network intrusion detection model based on 1DCNN-BiGRU. The 1DCNN and BiGRU models are used to obtain the spatial and temporal features of multimodal data, respectively, and the fusion of the spatial and temporal features of multimodal data is realized through the full connectivity layer, which then realizes the network intrusion detection of the emergency security response system. The study shows that the weighted average F1 score of the 1DCNN-BiGRU model in network intrusion detection is up to 0.9335, and the acceleration ratio of the emergency response system in the energy industry is up to 143.91, which can effectively realize the system dynamic load balancing. Fully exploiting the changing characteristics of multimodal data and integrating deep learning to promote the energy industry emergency safety response capability.

Index Terms Kubernetes, network intrusion detection, 1DCNN, BiGRU model, emergency security response

I. Introduction

Accompanied by the technological progress of advanced information technology and energy production, transmission, storage and other links, as well as the increasing expansion of market-based energy subjects, the interconnection of multiple energy sources, the trend of the plurality of subjects in the energy system has become more and more obvious, and the probability of systematic risk in the energy industry has increased significantly compared with the past [1]-[3]. The security risk faced by the energy industry not only involves the technical problems of the energy system itself, but is also closely related to external factors such as natural disasters and man-made attacks [4], [5]. Therefore, around the full range of energy safety and risk-related information, energy authorities should further smooth the channel of high quality and efficient information reporting, and seriously form a feedback mechanism for the risks reflected by frontline employees [6]-[8]. The establishment of a rapid disclosure system of accurate information in emergency situations, the triggering role of information for market mechanisms, and the enhancement of the initiative of energy emergency response [9], [10].

Emergency response usually refers to the preparations made to cope with the occurrence of various unforeseen events and the measures taken after the events [11]. The purpose of emergency response is to minimize the damage of security incidents and failures, and to monitor such incidents as well as learn from them, safeguarding the confidentiality, integrity and availability of information [12]-[14]. In fact, emergency information management in the energy industry mainly lies in the collection, storage, and distribution of information, which will be beneficial to the energy industry in the face of emergency security incidents can be the first time to complete the scheduling of resources for emergency response [15]-[17]. With the rapid development of big data technology, its powerful computing and analyzing capabilities provide new ideas for emergency security protection in the energy industry [18], [19]. Future work can further optimize the risk prediction model, improve the prediction accuracy in complex scenarios, and explore the introduction of multimodal data fusion technology into the emergency response decision-making process to enhance the intelligence of the system [20]-[22].

In order to effectively improve the emergency security response capability of the energy industry and better guarantee the transformation of the energy industry's emergency security response capability to intelligence, this paper proposes an emergency security response system for the energy industry based on the Kubernetes cluster management system. With the support of this system, this paper proposes a system network intrusion detection model based on 1DCNN-BiGRU. It extracts the spatial features of multimodal data through 1DCNN network,

introduces BiGRU model to obtain the temporal features of multimodal data, and realizes the effective fusion of the temporal and spatial features of multimodal data through the full connectivity layer, which is used in network intrusion detection. The effectiveness of the network intrusion detection model and the emergency security response system is simulated and analyzed in this paper.

II. K8s-based emergency safety response system for the energy industry

In the context of the new era of socio-economic development, the continuous innovation of network technology affects the development of all sectors of society. Among them, the informatization of energy industry has also been developed rapidly. On this basis, with the help of network technology to obtain the multimodal data of the energy industry, intelligent decision-making to assist the energy industry to realize the emergency safety response decision-making, to better ensure the safety performance of the energy industry in the process of informatization development.

II. A. Overall framework of the emergency security response system

II. A. 1) Kubernetes cluster management system

Kubernetes is an open source system for managing integrated applications across hosts in clusters. One of the core features of Kubernetes is that it dynamically manages containers to ensure that the state of the cluster meets the user's needs. In the Kubernetes cluster management system (K8s), all containers run inside Pods, and each Pod can run one or more containers. Containers inside each Pod are guaranteed to collaborate on the same machine and share resources, and each Pod can also have zero to multiple storage volumes, which can be a private directory for each container or a common directory inside the same Pod. On Kubernetes, users can create and manage Pods on their own [23].

Figure 1 shows the Kubernetes cluster management system framework. A Kubernetes cluster is functionally divided into a Master node and a Minion node, which can be either on the same host or on different hosts. The Master node runs the components that control the entire cluster, i.e., the Kube-APIServer, the Kube-Controller-Manager, and the Kube-Scheduler. There are two components on the Minion point, Kubelet and Kube-Proxy, which are responsible for running specific Pods and containers. In addition, the cluster needs an Etcd to store the current resource indexes in the cluster, which is a distributed key-value store component used for persistent storage.

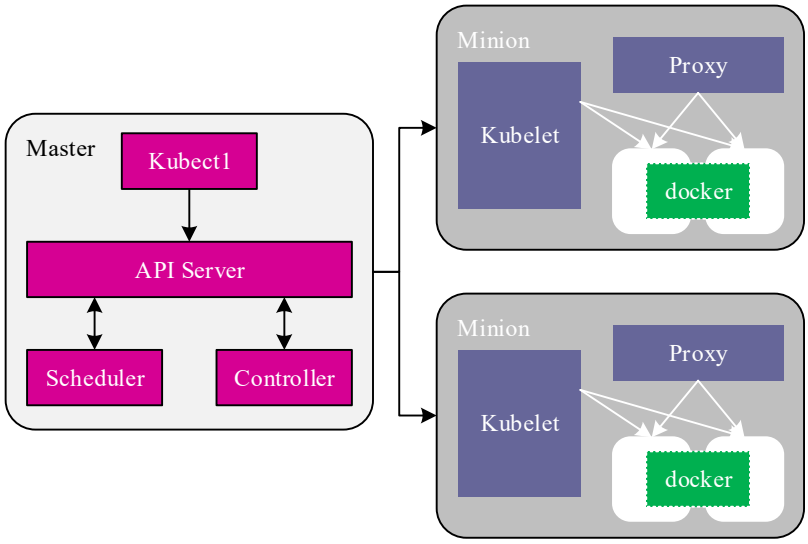


Figure 1: Kubernetes cluster management system framework

II. A. 2) Emergency security response system framework

In order to better realize the construction of energy industry emergency safety response system, this paper takes Kubernetes cluster management system as the basis, combines Pareto's law, multi-tier architecture idea and classification and grading idea, and establishes the energy industry emergency safety response system as shown in Figure 2. It mainly consists of two parts: on-site emergency response device and remote emergency support platform. The “up” part interfaces with the energy industry security data resource center to share key information such as ransomware samples and major security vulnerabilities. “Downstream” collects on-site data from the enterprises involved in the incident, including traffic data, log data, virus samples, infected files, and so on.

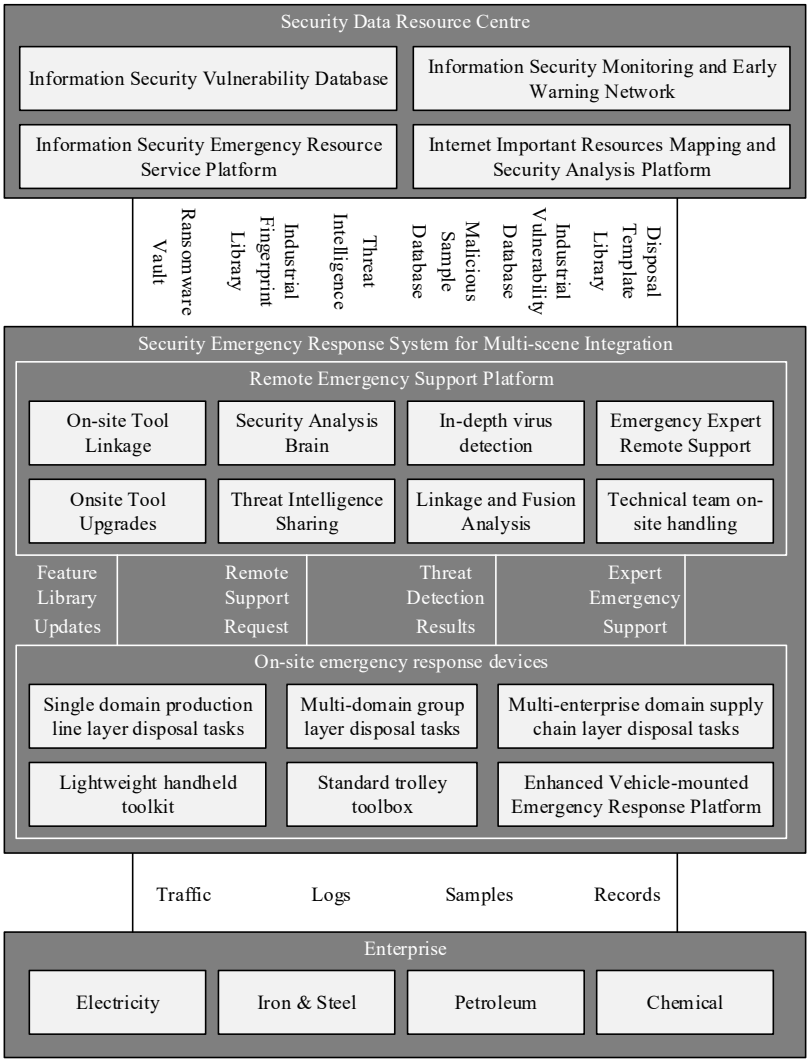


Figure 2: Framework of Emergency safety response system

The on-site emergency response device combines the relevant technical characteristics of the energy industry at the emergency site, and based on the “Preparation - Detection - Suppression - Eradication - Recovery - Summarization” general emergency response process issued by NIST, collects relevant data to carry out a series of actions such as event analysis, event diagnosis, attack localization, evidence fixation, and emergency response, and realizes the effective emergency response. Effective emergency response. Meanwhile, in the case of ineffective localization, through the linkage with the remote emergency support platform, it ensures the effective disposal of security incidents, reduces the impact on the on-site business and restores the production business in a timely manner.

The remote emergency support platform can be used as the core hub of a large-scale security incident emergency response system. The platform has a built-in threat detection engine, and through the docking management with on-site emergency response devices, it can realize remote emergency support and linkage scheduling, and can carry out fusion analysis of collected data. The platform is upwardly connected to the security data resource center to obtain security data resources from the information security vulnerability database, information security monitoring and warning network, and information security emergency resource service platform. It is also transformed into the feature database required by the on-site emergency response device, and can be pushed downward to realize the updating and upgrading of tools at any time, so as to improve the ability of network security threat detection and emergency response.

II. B.Functional design of the emergency security response system

II. B. 1) Data acquisition and monitoring

A network monitoring system monitors network traffic in real time through sensors distributed in the network to detect abnormal behavior and potential threats. The monitoring data can be expressed by the formula:

$$D_t = \sum_{i=1}^{N} x_i(t) \tag{1}$$

where D_t is the total amount of network traffic data at time t, N is the number of monitoring points, and $x_i(t)$ is the traffic data of the i th monitoring point at time t.

The log collection system is responsible for collecting and storing log data generated by network devices and security devices, providing detailed event tracking information. These log data are preprocessed and stored by the system to provide data support for subsequent event analysis. The storage and processing efficiency of log data is calculated by the formula:

$$E = \frac{D}{T} \tag{2}$$

where E is the processing efficiency, D is the amount of data processed, and T is the time required for processing.

The real-time alert system generates alerts in real-time by analyzing monitoring and logging data to alert personnel to potential security events. The system uses deep learning algorithms to analyze anomalous data and determines whether to generate an alert through a preset threshold, ensuring that potential threats can be detected and dealt with in a timely manner.

Through the collaborative work of the network monitoring system, log collection system and real-time alarm system, the data collection and monitoring module is able to realize efficient monitoring and timely warning of network security events, provide reliable data support for emergency security response management, and ensure intelligent management and efficient operation of the system.

II. B. 2) Network security detection

Emergency response teams need to use a variety of tools and techniques to detect and analyze threats. Threat detection usually requires the use of network auditing systems and intrusion detection systems, which can help the emergency response team to detect abnormal protocols and traffic in the network, such as a communication protocol that does not exist, or abnormal traffic generated by an IP access control system that does not exist.

Analyzing threats usually uses tools and technologies with functions such as network traffic analysis, system log analysis, malware analysis, etc., which facilitates the emergency response workgroup to understand the source, target, mode, and impact of the threat. At the same time, after the incident has already occurred, the emergency response working group needs to classify the level according to the impact of the incident and activate the emergency response plan. In case of a major or mega network and information security incident, it is required to report to the local industry authorities within one hour and provide a written report within two hours. It is strictly prohibited to release information on emergencies to the public without authorization, and the Emergency Disposal Command is responsible for guiding public opinion and providing the caliber of release.

II. B. 3) Emergency security response

The emergency response module is located at the core of the system and bears the important responsibility of rapid response and scientific decision-making after the occurrence of risks. The module consists of emergency plan library, knowledge reasoning engine, intelligent decision-making system and other components. Among them, the emergency plan library stores standardized disposal plans for different risk scenarios, covering the whole process of prevention, disposal and recovery. The knowledge inference engine adopts deep learning-based knowledge mapping technology, which can automatically match the optimal emergency response plan according to the specific situation of risk occurrence, and dynamically adjust and optimize the plan according to the inference results.

The workflow of emergency response is as follows: when the monitoring module discovers a potential risk or the prediction module warns that a risk is about to occur, the emergency response module starts immediately, and the knowledge reasoning engine starts to quickly diagnose and analyze the risk event and match the best disposal plan from the emergency plan library. At the same time, the intelligent decision-making system takes into account multiple factors such as the severity of the risk, grid operation status, site environmental conditions, etc., to optimize and adjust the emergency response plan and form the final execution plan.

The Response Execution Module is responsible for transforming the emergency decision plan into specific control instructions and sending the instructions to the intelligent execution unit on site. The module adopts industrial Ethernet and real-time communication protocols to ensure low latency and high reliability of instruction transmission.

The execution unit mainly includes various types of field devices in the energy industry, and realizes real-time control and autonomous decision-making at the device level through edge computing technology.

III. Network intrusion detection model incorporating multimodal data

The development of information and communication technology has improved the intelligent, unmanned, and refined control capabilities of the energy industry, however, it has also brought serious threats to the security of intelligent system networks in the energy industry. Therefore, it is crucial to utilize timely and accurate detection and identification methods in order to control and prevent intrusions that threaten energy industry system networks. Intrusion detection is a typical active defense technology, which is one of the important research topics in the field of computer network security, and has been widely used in information physics systems, smart grids, smart cars, etc. To this end, this paper proposes a network intrusion detection model for 1DCNN-BiGRU model for multimodal data fusion, which aims to enhance the accuracy and efficiency of network intrusion detection for emergency security response systems in the energy industry.

III. A. Deep Learning Related Technologies

III. A. 1) Convolutional Neural Networks

Convolutional Neural Networks (CNNs) mainly contain a convolutional layer, a pooling layer and a fully connected layer. In the convolutional layer, the input image is convolved with a series of convolutional kernels with linear displacement invariance through convolutional operations to capture spatial contextual information in the image. The pooling layer, on the other hand, employs techniques such as mean pooling or maximum pooling to compress the spatial dimensions of the feature map to extract generic and abstract features. The fully connected layer converts these features into feature vectors for the final classification task. After the model is constructed, it is trained by an optimizer. During the training process, the difference between the predicted value and the true value is measured by the backpropagation algorithm, the weights and biases are updated by using the objective function back-propagation error, and the algorithms such as stochastic gradient descent are used to iterate repeatedly [24].

(1) Convolutional layer. The convolutional layer is the core component of the CNN, which achieves local feature extraction from the input data through convolutional operations. The sliding operation of the convolution kernel enables the network to capture the spatial structure information in the input data, and through the parallel use of multiple convolution kernels, the network can learn the representations of different features.

(2) Pooling layer. The pooling layer can be used to reduce the spatial dimensionality of the data, decrease the computational complexity, and enhance the robustness of the model. For a given sensory field region, maximum pooling takes the maximum value within the region as the output, then:

$$Max\ Pooling(X) = \max(X) \tag{3}$$

where X is the input data within the receptive field.

Average pooling takes the average of all elements in the receptive field as the output, then:

$$Average\ Pooling(X) = \frac{1}{size}\sum_{i=1}^{size} X_i \tag{4}$$

where X_i is each element within the receptive field and $size$ is the size (number of elements) of the receptive field.

(3) Batch Normalization Technique. Batch normalization (BN) aims to speed up the training process of neural network and improve the stability of the model, batch normalization pulls the input values of the hidden layer neurons back to a standard normal distribution with a mean of 0 and variance of 1 by normalizing the data in each small batch [25]. Its mathematical expression is:

$$BN(x) = \gamma \frac{x-\mu}{\sqrt{\sigma^2+\varepsilon}} + \beta \tag{5}$$

where x is the input data, μ and σ are the mean and standard deviation of a small batch of data, respectively, γ and β are the learnable scaling and translation parameters, and ε is a small constant used to avoid the case where the root is zero.

(4) Fully connected layer. A fully connected layer is a basic type of network layer in deep learning neural networks, in which each neuron is connected to all neurons in the previous layer to form a fully connected network structure. This means that each neuron of the fully connected layer receives all the outputs of the previous layer and inputs them as a weighted sum of weights to the current layer. The structure of a fully connected layer can be represented as:

$$y_i = f\left(\sum_{j=1}^{N} w_{ij}x_j + b_i\right) \tag{6}$$

where y_i is the output of the i th neuron of the current layer, x_j is the output of the j th neuron of the previous layer, w_{ij} is the weight connecting these two neurons, b_i is the bias term of the current neuron, and f is the activation function.

III. A. 2) Door control cycle units

Gated Recurrent Unit (GRU) is a type of network in Recurrent Neural Network (RNN) and also a variant of Long Short-Term Memory Neural Network (LSTM).GRU replaces the input gate, forgetting gate, and output gate in LSTM with reset gate and update gate [26]. Compared to LSTM, GRU has one less gate function, fewer parameters, and a simpler network structure, which allows for faster convergence when training the model.

In the GRU cell cell structure, x_t and h_{t-1} are the inputs and h_t is the output. x_t is the current input and h_{t-1} is the hidden state, i.e., the output of the previous cell. z_t represents the update gate, r_t represents the reset gate, and $\tilde{h}_t$ represents the candidate state information. The update gate z_t decides whether to update the hidden state h_{t-1} to the current state h_t, which can be expressed as:

$$z_t = \sigma(W_s \times [h_{t-1}, x_t]) \tag{7}$$

where σ is the sigmoid function and W_s is the weight parameter.

The reset gate r_t determines whether the hidden state h_{t-1} is reset or not and can be expressed as:

$$r_t = \sigma(W_r \times [h_{t-1}, x_t]) \tag{8}$$

where W_r is the weight parameter.

$\tilde{h}_t$ and h_t record historical information about the data, which can be expressed as:

$$\tilde{h}_t = \tanh(W_r \times [r_t \times h_{t-1}, x_t]) \tag{9}$$

$$h_t = (1 - z_t) \times h_{t-1} + z_t \times \tilde{h}_t \tag{10}$$

The bi-directional gated recurrent unit (BiGRU) consists of two ordinary GRUs that process the input sequence along the time forward sequence and time inverse sequence, respectively, fusing their respective outputs as the result. Since BiGRU can process both forward and reverse order information of data, BiGRU can capture more feature information and has higher performance compared to ordinary GRU.

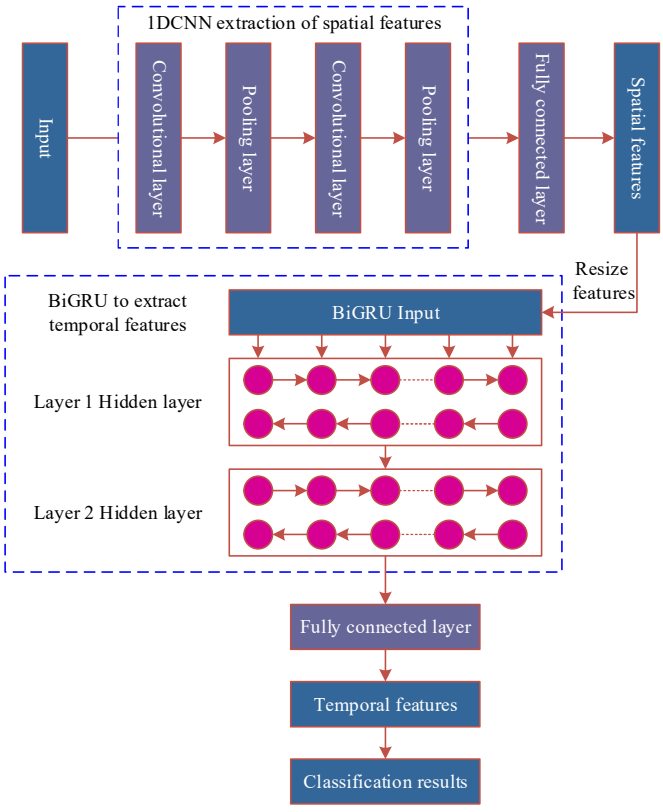


Figure 3: 1DCNN-BiGRU model structure diagram

III. B. 1DCNN-BiGRU Modeling and Processes

III. B. 1) 1DCNN-BiGRU modeling

Given that the current intrusion detection data has a small number of samples of intrusion behaviors, resulting in an unbalanced distribution of data categories, this paper uses the training dataset to increase the number of intrusion behaviors data in the training samples through feature sampling techniques, thus mitigating the impact of data imbalance on the detection accuracy.

1DCNN is specially used to deal with one-dimensional sequence data, which can automatically capture spatially localized features in the sequence, and at the same time has good computational efficiency, and can automatically extract features from the original data, thus reducing the difficulty of feature engineering, and the model has stronger generalization ability and adaptability.BiGRU has better memory ability and generalization ability, and it can better deal with the sequence data, and can effectively alleviate the problem of gradient vanishing. Both are able to extract spatial and temporal features at the same time, thus making full use of feature information and thus improving the accuracy of the model. Figure 3 shows the network intrusion detection model based on 1DCNN-BiGRU. This structure utilizes the feature extraction and pooling capabilities of 1DCNN to capture both local and global features of multimodal data, and then better understands and exploits the temporal information of the sequential data through the sequence modeling capabilities of BiGRU network. Finally, the multimodal data fusion is performed through the fully connected layer and SoftMax function, and the learned features are mapped to categories for effective classification.

III. B. 2) Network Intrusion Detection Process

The 1DCNN-LSTM model mainly consists of three basic modules, i.e., data preprocessing module, training module, and classification module. The steps of using it to carry out network intrusion detection in the energy industry emergency security response system are as follows:

Step1 Acquire multimodal data using the acquisition module of the energy industry emergency security response system.

Step2 Data preprocessing is the basic collection of data sets, which is used to characterize normal data and form a feature data set as the basis for subsequent network intrusion judgment and classification. And the preprocessed data is divided into two parts, training set and test set, according to the ratio of 7:3.

Step3 In the training module, through the convolution construction of network intrusion judgment features in the massive data, the feature function is further fixed, and then the model can realize the purpose of efficient detection of data packets.

Step4 The classification module, as the result output module of network intrusion recognition, realizes the output of the results by interacting with the test set and validation set, and analyzes the performance of the model by using many different types of evaluations, so as to safeguard the network security of the emergency security response system in the energy industry.

IV. Network intrusion detection and emergency security response system testing

The traditional energy industry is undergoing a dramatic evolution towards intelligence, which is based on integrated, high-speed and bi-directional communication networks that enable safer and more efficient energy management through advanced sensing and measurement technologies, advanced control methods and big data technologies. Extensive communication infrastructures have been used to transmit and monitor operational parameters at energy system connection points. However, the openness of the network also makes energy industry intelligent systems more vulnerable to various malicious cyber attacks. How to realize the cybersecurity of emergency security response systems in the energy industry has become a key and hot research area nowadays.

IV. A. Valid validation of the 1DCNN-BiGRU model

IV. A. 1) Network Intrusion Detection Effectiveness

In this section, the validation of the 1DCNN-BiGRU model is carried out using the CICIDS dataset, which contains eight types of network intrusions, namely, Benign, Botnet, Brute Force, Distributed Denial of Service (DDos), Denial of Service (Dos), Unauthorized Access Intrusion (Infl), Port Scanning, and Web Attacks. (Infl), Port Scanning Attacks (Port), and Web Attacks, which are eight types of network intrusions.

The learning rate of 1DCNN-BiGRU model is set to 0.0001, the number of iterations is 100 epochs, and precision, recall, F1 score, and confusion matrix are selected as the evaluation metrics to obtain the metrics of 1DCNN-BiGRU model on the CICIDS dataset as shown in Table 1, and the confusion matrix is shown in Figure 4. The underlined lines in the table indicate the intrusion types with relatively low performance in intrusion detection metrics.

Based on the results of the experiments analyzing the confusion matrix and the various metrics of the model on the CICIDS dataset, the following conclusions can be drawn:

Botnet and Dos have relatively poor classification results, where the precision and recall of Botnet are low, probably due to the small number of samples, which makes it difficult to differentiate. The lower recall of DDos and Dos may be due to the fact that these two types of attack traffic are less frequent in real network environments, with fewer and more rapidly changing sample sizes. In addition, the Port category has a high false positive rate, which requires further model optimization.

Overall, the 1DCNN-BiGRU model has an accuracy of 0.9301 on the dataset and a weighted average F1 evaluation score of 0.9335, with recall, precision and F1 evaluation scores given for each category. In the weighted average metric, the precision and recall of the 1DCNN-BiGRU model are 0.9302 and 0.9348, respectively, which indicates that the algorithm has a good performance in balanced classification of attack and normal traffic, and is able to effectively classify attack and normal traffic in the dataset.

However, the performance of the model needs to be improved for some cases where the number of attack type samples is small or the features are difficult to distinguish. Therefore, subsequent methods such as optimizing feature selection or tuning the model may be needed to improve the classification performance for Botnet, Dos and Port attacks. In addition, the analysis of the confusion matrix and various metrics of the test set can help researchers to understand the performance of the model on different categories and optimize and improve based on these results. In summary, the CICIDS dataset is a complex dataset, which puts high requirements on the model's classification ability and generalization ability, but the 1DCNN-BiGRU model has a better performance on this dataset, which provides a certain reference value for the research and application of network intrusion detection in the emergency security response system in the energy industry.

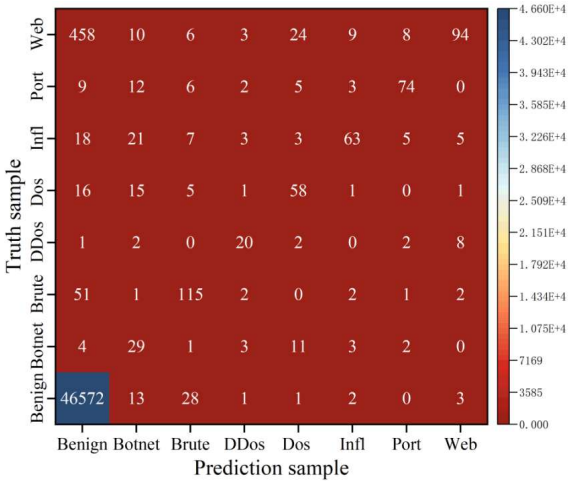


Figure 4: Confusion matrix of CICIDS dataset

Table 1: Indicators of 1DCNN-BiGRU in CICIDS dataset

Type	Precision	Recall	F1 score	Number
Benign	0.9463	0.9768	0.9657	47129
Botnet	0.6512	0.4631	0.5248	103
Brute	0.8537	0.8252	0.8343	168
DDos	0.8142	0.5367	0.6735	35
Dos	0.6905	0.4034	0.5011	104
Infl	0.8914	0.7392	0.8142	83
Por	0.8046	0.4513	0.5563	92
Web	0.7438	0.6478	0.7038	113
Macro avg	0.7995	0.6304	0.6967	47827
Weight avg	0.9302	0.9348	0.9335	47827
Accuracy	0.9278			

IV. A. 2) Comparison results of different models

Based on the performance examination of the 1DCNN-BiGRU model in the previous subsection, this paper further develops the validation from the model performance comparison. The CICIDS dataset is still taken to train the model, and the performance of the 1DCNN-BiGRU model is compared with other imbalance algorithms, traditional algorithms and deep learning algorithms. The accuracy rate (ACC), correct detection rate (CDR), and false alarm rate are selected as evaluation metrics (FAR), and the comparison results of different models are obtained as shown in Table 2.

Compared with other unbalanced learning methods, the 1DCNN-BiGRU model proposed in this paper uses the least number of samples to obtain the best performance. In terms of accuracy and correct detection rate, I-NGSA and CANN+SMOTE models achieve better results in imbalance learning models. In contrast, the 1DCNN-BiGRU model proposed in this paper is slightly less effective than the above two models, but since both achieve more than 99% detection rate. So the disadvantage of this part can be ignored and can be regarded as a better detection level.

Compared with shallow learning, GA-LR performs well in all the indicators in shallow learning, and the overall effect is slightly better than the 1DCNN-BiGRU model proposed in this paper. However, since the size of the training dataset required by the GA-LR model is about six times that of the present model. Therefore, under the same amount of data, the convergence of this model is better than the GA-LR model. It shows that the present algorithm is optimal with a small amount of data.

Compared with other deep learning models, the results show that all other deep models have better performance. Among them, the CNN-LSTM and DNN models have overall better detection than the present model, have the same problem as the GA-LR model, and require much more data than the present model.The S-NADE model, with overall worse performance, requires much more data than the present model.The SCDNN model, with a very low correct detection rate.

Combining the above results, it can be seen that the 1DCNN-BiGRU model established in this paper has better detection performance when performing network intrusion detection, and its application to the energy industry emergency security response system can significantly enhance the detection accuracy of abnormal network intrusion traffic and better ensure the network security of the energy industry emergency security response system.

Table 2: The comparison results of different models

Algorithm		ACC/%	CDR/%	FAR/%	Dataset size
Unbalanced algorithm	CANN+SMOTE	98.42	99.53	0.561	121463
	MHCVF	98.15	95.45	1.359	504932
	DENDRON	97.63	95.82	1.072	125918
	I-NGSA	99.29	99.37	--	125918
	1DCNN-BiGRU	98.31	99.06	0.115	72536
Traditional algorithm	SVM	94.35	92.86	3.632	145855
	OS-ELM	98.62	99.07	1.517	125918
	TLMD	93.23	93.42	0.815	88604
	GA-LR	99.71	99.15	0.176	434152
	1DCNN-BiGRU	99.15	98.83	0.128	72536
Deep learning algorithm	CNN+LSTM	99.65	97.63	0.062	2516834
	S-NADE	97.38	97.18	2.238	434152
	DNN	99.62	99.74	0.935	125918
	SCDNN	92.35	92.59	7.764	63709
	1DCNN-BiGRU	99.27	98.76	0.101	72536

IV. B. Performance testing of the security emergency response system

IV. B. 1) Correctness and efficiency tests

The monthly data of a power grid for the month of August 2023 is used as the basis to simulate the network intrusion behaviors present in it. Under regular single-core computation, it takes more than 3 hours. In the platform of this paper, the Kubernetes cluster management configuration is changed through the Kubernetes cluster management configuration of parallel digits 1~150, to obtain its computation time consuming and acceleration ratio as shown in Figure 5. The acceleration ratio is defined as the ratio of serial execution time to parallel execution time.

The acceleration ratio basically shows a linear increase as the number of cores and the degree of parallelism increase. With 150 cores provided, it only takes about 58.74s to complete the computational task of grid network intrusion behavior detection, which takes 3 hours in the traditional case, and its acceleration ratio is even as high

as 143.91. This value is close to the theoretical optimum considering the delay in task scheduling. The above results show that the emergency safety response system of the energy industry established in this paper combined with the Kubernetes cluster management system has extremely superior simulation efficiency, which can effectively improve the simulation speed of the energy system after large-scale data access, shorten the simulation time of multiple faults in a certain way to the simulation time of a single fault, realize the online deployment of traditional offline simulation tools, and realize the transformation from scientific research tools to production tools.

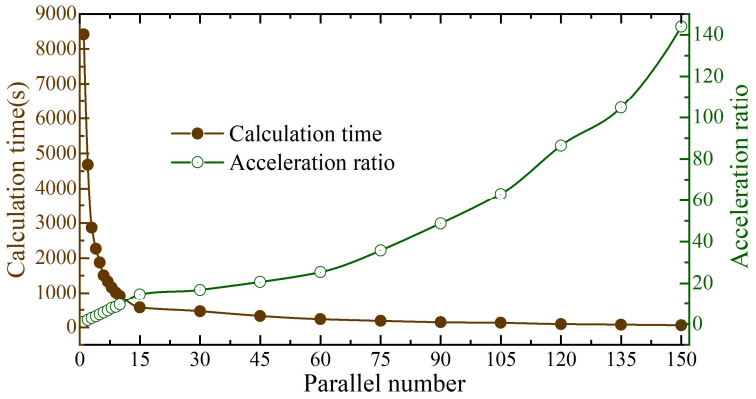


Figure 5: Parallel efficiency test

The correctness referred to in this article refers to the difference between the calculation using this platform and the conventional stand-alone calculation, rather than whether the core computing engine itself calculates correctly or not. After testing in different scenarios, the platform-based calculation and the conventional stand-alone calculation are completely consistent, and the curves are completely overlapping. In addition, this paper verifies the reliability of the system, and manually shuts down all K8s cluster master servers and restarts them during the simulation process. In the test, the "Fault Tolerant Service", "Provisioning Service", etc., are restarted normally, and the tasks that are not executed or not completed are recalculated. During the simulation, the messages in the "To be Computed" queue are directly consumed by a forged client, causing the normal provisioning service to fail to obtain the messages normally. The test result shows that the Fault Tolerance Service of the scheduled scan finds that the task has not been completed after the timeout in OSS and is not in the "To be calculated" or "To be processed" team, that is, it generates a message of "To be calculated" for the task, and then executes it according to the normal process.

IV. B. 2) Dynamic load balancing mechanisms

The energy industry emergency security response system designed in this paper is built based on Kubernetes cluster management system, which can effectively realize system dynamic load balancing and ensure emergency response resource scheduling of the energy industry emergency security response system. In order to verify its scheduling performance, this paper uses the control variable method to analyze its dynamic load balancing mechanism. That is, the experimental group uses the Kubernetes cluster management system for emergency response resource scheduling, and the control group does not use the system for scheduling. The specific experimental steps are as follows:

(1) Both experimental groups create 10 GuestBook applications to the APIServer of the cluster through the client, including two each of three restart policies and two resource quality of service, and the values of the requests of each application are as different as possible. Such 10 applications are then created every 15 minutes until 50 GuestBook applications are created.

(2) Install the Webbench tool on the client side. Webbench is a well known web site stress testing tool, Webbench can simulate up to 50,000 concurrent links to test the load capacity of a web site, and can also concurrently make random requests to some services. Here we use it to work in parallel to the nodes to send Web requests, the number of requests generated by a random function. It is used to test and observe the change in score of cluster services under high load.

(3) Monitor and record the resource usage of each node on the Master node, record once when the GuestBook is just created, and once after 10 minutes of creation, and once after the application is just created in order to understand the immediate load of the node when the application is created. Recorded 10 minutes after the creation

of the application, that is, before the next time to create the application, this time the record is to observe the node load after a period of time in the application service.

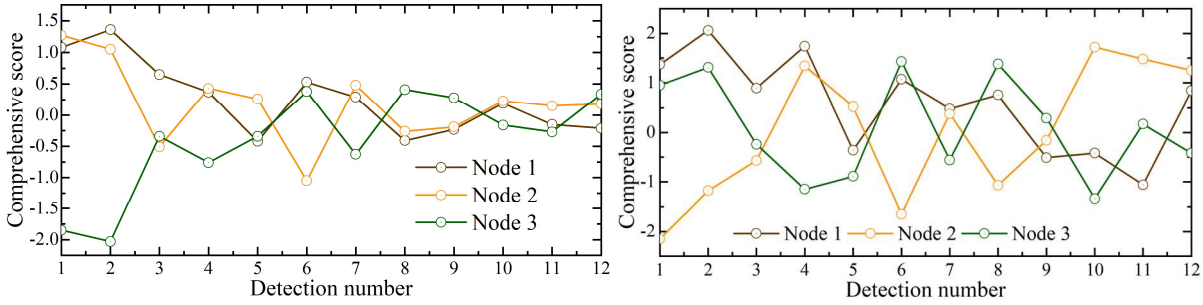
(4) Timed dynamic load balancing, which is performed 10 minutes after the application is created.

(5) Observe and output the monitored load score data.

(6) Calculate and analyze the obtained data.

In this paper, a total of 12 detections are carried out, and the composite scores on each node are shown in Fig. 6, where Fig. 6(a)~(b) shows the composite scores of the experimental and control groups, respectively.

Since the number of Pods is small in the first two detections, it is easy to see that the accesses are concentrated in a certain node, so it is seen that the scores of the first two detections of the nodes in the experimental group are more dispersed, i.e., the node loading is extremely unbalanced. Due to the dynamic load balancing in the cluster operation, the score of the nodes in the cluster gradually tends to 0 in the later detection, i.e., the load tends to be balanced. We can calculate the standard deviation of the scores of each node in the cluster at each detection, and use this standard deviation as a quantitative value of the degree of stability of the cluster at this moment. The average of the standard deviation of each detection is used as the quantitative value of the degree of stability during this detection time. It is calculated that the quantized value of stability of the experimental group is 0.572 during this detection time.In the control group without using Kubernetes default scheduling algorithm, also the first two accesses are more scattered due to the fact that the number of Pods in the first two detections is less and the accesses appear to be concentrated in a certain node. However, relatively speaking, the overall comprehensive score of the control group that does not use the Kubernetes default scheduling algorithm has a larger overall fluctuation, which indicates that there are large fluctuations in its choice of node resources, which can easily lead to the system becoming unbalanced in terms of load. The quantitative value of the stability of the control group is calculated to be 0.988 during this testing time, which is 72.73% higher than that of the experimental group, which fully demonstrates the feasibility of the Kubernetes cluster scheduling algorithm.



(a) The experimental group (b) The control group

Figure 6: The comprehensive scores of each node

V. Conclusion

In order to enhance the emergency security response capability of the energy industry, this paper establishes an emergency security response system for the energy industry based on the Kubernetes cluster management system, and designs a network intrusion detection model based on 1DCNN-BiGRU to improve the network security of the emergency security response system for the energy industry. Through the model effectiveness and system performance analysis, it is found that the accuracy and weighted average F1 evaluation score of the 1DCNN-BiGRU model on the dataset reach 0.9301 and 0.9335, respectively, and the emergency security response system designed in this paper can complete the computational task of network intrusion detection in only about 58.74s with the provision of 150 cores. Combined with the default scheduling algorithm of Kubernetes cluster management system to carry out the scheduling of emergency resources, the dynamic load balancing of the system can be realized, and the rapidity, stability and reliability of the system response can be better ensured.

References

[1] Burgherr, P., Giroux, J., & Spada, M. (2015). Accidents in the energy sector and energy infrastructure attacks in the context of energy security. European Journal of Risk Regulation, 6(2), 271-283.

[2] Szulecki, K., & Kusznir, J. (2018). Energy security and energy transition: securitisation in the electricity sector. Energy security in Europe: divergent perceptions and policy challenges, 117-148.

[3] Chernyaev, M. V., & Rodionova, I. A. (2017). Analysis of sustainable development factors in fuel and energy industry and conditions for achievement energy efficiency and energy security. International Journal of Energy Economics and Policy, 7(5), 16-27.

[4] Jia, Y., Xu, Z., Lai, L. L., & Wong, K. P. (2015). Risk-based power system security analysis considering cascading outages. IEEE Transactions on Industrial Informatics, 12(2), 872-882.
[5] Ciapessoni, E., Cirio, D., Kjølle, G., Massucco, S., Pitto, A., & Sforna, M. (2016). Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties. IEEE Transactions on Smart Grid, 7(6), 2890-2903.
[6] Kang, K., Liu, Y. Y., Zhang, L. S., Bi, Q., He, L. K., & Zhang, Y. Y. (2023, October). Research on Business Center Monitoring System Based on Business Emergency System of Power Grid Company. In 2023 5th International Conference on System Reliability and Safety Engineering (SRSE) (pp. 389-394). IEEE.
[7] Zhang, K., Wang, L., Liu, J., Wu, H., Xu, X., Huang, D., ... & Liu, J. (2022). Resilience Capacity Evaluation for the Safety Management System of Power Grid Enterprise Based on AHP‐MEE Model. Mathematical Problems in Engineering, 2022(1), 8065814.
[8] Prokhorova, V., Budanov, M., & Budanov, P. (2024). DEVISING AN INTEGRATED METHODOLOGY FOR ENERGY SAFETY ASSESSMENT AT AN INDUSTRIAL POWER-GENERATING ENTERPRISE. Eastern-European Journal of Enterprise Technologies, 130(13).
[9] Hrinchenko, H., Prokopenko, O., Shmygol, N., Koval, V., Filipishyna, L., Palii, S., & Cioca, L. I. (2024). Sustainable energy safety management utilizing an industry-relative assessment of enterprise equipment technical condition. Sustainability, 16(2), 771.
[10] Zhao, X., Yang, H., Li, S., Li, Y., Yi, L., & Zhang, D. (2022, September). Emergency Material Supply for Power Enterprises Based on Internet of Things under Short-Term Prediction of Echo State Network. In 2022 3rd International Conference on Advanced Electrical and Energy Systems (AEES) (pp. 527-531). IEEE.
[11] Damaševičius, R., Bacanin, N., & Misra, S. (2023). From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management. Journal of Sensor and Actuator Networks, 12(3), 41.
[12] Pervez, F., Qadir, J., Khalil, M., Yaqoob, T., Ashraf, U., & Younis, S. (2018). Wireless technologies for emergency response: A comprehensive review and some guidelines. Ieee Access, 6, 71814-71838.
[13] Wu, W., Hou, H., Zhu, S., Liu, Q., Wei, R., He, H., ... & Luo, Y. (2024). An intelligent power grid emergency allocation technology considering secondary disaster and public opinion under typhoon disaster. Applied Energy, 353, 122038.
[14] Zhou, Q., Shahidehpour, M., Yan, M., Wu, X., Alabdulwahab, A., & Abusorrah, A. (2019). Distributed secondary control for islanded microgrids with mobile emergency resources. IEEE Transactions on Power Systems, 35(2), 1389-1399.
[15] Shi, Z., Xu, Y., Wang, Y., He, J., Li, G., & Liu, Z. (2022). Coordinating multiple resources for emergency frequency control in the energy receiving-end power system with HVDCs. IEEE Transactions on Power Systems, 38(5), 4708-4723.
[16] Kang, J. S., & Lee, S. J. (2022). Concept of an intelligent operator support system for initial emergency responses in nuclear power plants. Nuclear Engineering and Technology, 54(7), 2453-2466.
[17] Fishov, A., Osintsev, A., Ghulomzoda, A., Marchenko, A., Kokin, S., Safaraliev, M., ... & Zicmane, I. (2023). Decentralized Emergency Control of AC Power Grid Modes with Distributed Generation. Energies, 16(15), 5607.
[18] Qian, L., Bai, Y., Wang, W., Meng, F., & Chen, Z. (2023). Natural gas crisis, system resilience and emergency responses: A China case. Energy, 276, 127500.
[19] Dong, X., Wang, Y., Dang, X., Hu, T., Wang, Q., Li, H., ... & Sun, H. (2024, December). Research on Risk Analysis and Emergency Response Methods of Power Grid Operation in Cities. In 2024 5th International Conference on Power Engineering (ICPE) (pp. 559-566). IEEE.
[20] Li, J., Hou, Y., Cheng, X., Yan, X., & Chen, G. (2020, March). The On-duty Response Management System for Power Emergency Events based on Big Data Technology. In 2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS) (pp. 647-650). IEEE.
[21] Song, H., Tan, L., Chen, G., Wang, B., Cao, L., & Zhang, Y. (2025, March). Application of big data technology in optimizing emergency response to power grid disasters. In International Conference on Physics, Photonics, and Optical Engineering (ICPPOE 2024) (Vol. 13552, pp. 390-397). SPIE.
[22] Wu, W., & Yan, L. (2023, May). Evaluation Algorithm of In-Plant Emergency Management Capability for Nuclear Power Emergency Incidents Based on Big Data. In 2023 International Conference on Networking, Informatics and Computing (ICNETIC) (pp. 54-58). IEEE.
[23] Nikita Ramachandra & Rajasekar Natarajan. (2025). Kubernetes and IoT-based next-generation scalable energy management framework for residential clusters. Journal of Building Engineering,104,112292-112292.
[24] Fares Al Mohamad,Leonhard Donle,Felix Dorfner,Laura Romanescu,Kristin Drechsler,Mike P Wattjes... & Keno Kyrill Bressem. (2025). Open-source Large Language Models can Generate Labels from Radiology Reports for Training Convolutional Neural Networks. Academic radiology,32(5),2402-2410.
[25] Amelia E.H. Bridges,Eleanor Cross,Kyran P. Graves,Nils Piechaud,Antony Raymont & Kerry L. Howell. (2025). Practical application of artificial intelligence for ecological image analysis: Trialling different levels of taxonomic classification to promote convolutional neural network performance. Ecological Informatics,88,103146-103146.
[26] Wenhan Qu,Yintang Wen,Ning Yao,Yuyan Zhang & Xiaoyuan Luo. (2025). Ultrasonic nondestructive testing for composite bonded structures based on convolutional neural network and bidirectional gated recurrent unit (CNN-BiGRU) optimized by attention mechanism. The Review of scientific instruments,96(4).