

## RESEARCH ARTICLE

# An Improved Algorithm for Network Intrusion Detection Based on Deep Residual Networks

XUNTAO HU<sup>1</sup>, XIANCAI MENG<sup>2</sup>, SHAOQING LIU<sup>1,2</sup>, AND LIZHEN LIANG<sup>2</sup><sup>1</sup>Anhui University of Science and Technology, Huainan 232001, China<sup>2</sup>Institute of Energy, Hefei Comprehensive National Science Center, Hefei, Anhui 230031, China

Corresponding author: Shaoqing Liu (liushaoqing@ie.ah.cn)


This work was supported in part by the Institute of Energy, Hefei Comprehensive National Science Center under Grant 21KZS202 and Grant 21KZS208; in part by the National Natural Science Foundation of China under Grant 12105135; in part by the University Synergy Innovation Program of Anhui Province under Grant GXXT-2022003, Grant GXXT-2022-004, and Grant GXXT-2022-005; and in part by the Nature Science Foundation of Anhui Province under Grant 2308085MA22.

**ABSTRACT** The goal of current research will be to increase the accuracy and generalisation capacity of intrusion detection models in order to better handle the complex network security issues of today. In this paper, a new hybrid attention mechanism is introduced along with an enhanced algorithm. Through the effective channel layer and curve space layer, the feature information will be concentrated on the necessary feature information, allowing the model to concentrate more on the features linked to classification and become more broadly applicable. Increase the model's precision. The experimental results demonstrated that the accuracy can achieve 100%, 99.79%, and 98.10% on binary classification problems and 96.37%, 98.12%, and 99.06% on multiclassification problems, respectively, using the UNSW-NB15, CICIDS-2017, and CICIDS-2018 datasets for validation.

**INDEX TERMS** Intrusion detection, residual networks, hybrid attention mechanisms, bidirectional long and short memory networks.

## I. INTRODUCTION

The Internet has become an indispensable productivity tool in human life as the rapid development of Internet technology continues to change the way of life for mankind [1], [2]. As an extension of the Internet, the IoT connects various smart devices together to build an intelligent and interconnected ecosystem. However, in this highly interconnected network environment, people face numerous cybersecurity problems [3], [4]. Various cyber-attacks are emerging; the size of the network is increasing [5], and the frequency of attacks is climbing. These challenges put the security of IoT to a severe test. Network intrusion detection Technology is particularly important in this context. It accurately detects various network attacks by detecting and analysing the data in IoT in order to discover the presence of unusual forms of information. Intrusion detection has thus become one of the most popular research directions in the field of IoT

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood .

security [6], [7]. However, traditional intrusion detection techniques suffer from low accuracy [8], a problem that may become even worse in the IoT environment. In order to tackle this challenge, intrusion detection algorithms Techniques need to be continuously improved to address the characteristics of IoT and the complexity of the network environment. Utilising the communication characteristics and data We design a more intelligent and efficient intrusion detection system based on the transmission patterns between IoT devices. Simultaneously, the design incorporates advanced technologies like machine learning, and artificial intelligence are combined to improve the ability of the intrusion detection system to recognise abnormal data in order to improve accuracy and timeliness [9], [10]. In the era of the Internet of Things (IoT), improving the accuracy of intrusion detection technology is not only a top priority in network security research but also one of the keys. to ensure the stable operation of the IoT ecosystem. Through continuous research and innovation, people's information security can be better protected. Reference [11] and [12] and The healthy

development of IoT technology can be promoted. The depth of the study and the increasing complexity of the network model make it challenging to manage the conventional machine learning model for high-precision network intrusion detection. Researchers started using deep learning models for intrusion detection, such as convolutional neural networks, recurrent neural networks, artificial neural networks, and so on, in order to increase the accuracy of model detection. In a convolutional neural network, various feature information can be learned by various convolutional layers, and these features can be combined to obtain accurate information about the target object, which suggests that the accuracy of feature extraction has a significant influence on the classification outcomes. With the wide variety of features in intrusion detection datasets, it becomes very difficult to extract the key information. Therefore, to address the above problems, this paper proposes a hybrid hyperbolic residual extraction feature method that introduces a new hybrid attention mechanism. The hybrid attention module is a combination of an efficient channel attention mechanism and a hyperbolic residual linked spatial attention mechanism, which reduces the compression of features in the channel dimension and improves accuracy compared to the CBAM (convolutional attention) mechanism. On top of the spatial module, using hyperbolic residual attention, the bidirectional curvilinear convolution kernel adjusts the corresponding weights according to the geometric relationship to better capture the feature information in space. The residual connection prevents the model layers from being too deep, which leads to incomplete feature information extraction. Reduces the accuracy of the model. The pre-processed data features are inputted into the module, and the attention to different features is dynamically adjusted through network adaptive learning of the importance of different features and the importance of their impact on classification, so that the positive aspects have a greater impact on the model and the negative effects of redundant features on the model are weakened to improve the accuracy and generalization ability of the model. Our contributions are as follows:

- (1) A hybrid channel information extraction module is proposed to enable the model to focus on positive information more accurately, reduce the learning of redundant features, and improve the accuracy of the model.

- (2) proposes a combination of residual network and bi-directional long and short memory network, which can effectively classify the extracted information and improve the model's ability to generalize.

- (3) Lastly, experiments are run on the UNSW-NB15, CICIDS2017, and CICIDS2018 datasets and compared with several models.

The results of the experiments show that the model in this paper is better than the current mainstream models on the dataset. The remainder of the paper is arranged as follows: The presentation of pertinent techniques and associated models employed by current researchers is covered in Section II. The optimisation model's structure and associated

algorithmic knowledge based on the hybrid attention mechanism are provided in Section III. Section IV delineates the model's detection performance and the interpretation of the categorisation outcomes. Ultimately, the entire paper is summarised in Section V.

## II. RELATED WORK

One of the most frequently used systems for detecting network security, identifying malicious network traffic and computer usage that traditional firewalls are unable to detect, and maintaining the security of computer systems is the intrusion detection system (IDS). The importance of protecting property security and personal information cannot be overstated. Therefore, current research focuses on how to effectively and precisely identify hostile invasions. A variety of traditional machine learning algorithms have been successfully applied to all aspects of intrusion detection with the continuous development of machine learning for decades, but due to the increasing complexity of the network, the traditional machine learning algorithms are challenging to handle. After machine learning, deep learning has made significant strides in recent years and is now being explored and used in many important study fields. ElSayed et al. [13] came up with a new regularization method called SD-Reg, which is based on the standard deviation of the weights, to deal with the problem of overfitting and make it easier for the model to find unlabeled attacks. This method is highly effective for detection. In their deep learning model, Sinha et al. [14] combined bi-directional long and short memory networks with convolutional neural networks. Preprocessing the data before feeding it into the model enables it to learn the spatial and temporal characteristics of the data by combining the benefits of convolutional networks and bi-directional long and short memory networks. The model detects data with a high rate and produces few false positives. In order to perform classification, Nguyen et al. [15] combined bagging classifiers (BG) and convolutional neural networks, and the results of their classification were highly reliable. Their classification was validated using the KDD dataset and was based on exhaustive search and fuzzy C-mean clustering of genetic algorithms. Researchers Gan et al. [16] proposed an intrusion detection method based on the data imbalance of a convolutional neural network to address the issue of data imbalance by dividing a small number of samples made larger by attacks into a larger number of samples, using focal loss to compute the loss of the actual value and the expected value, and conducting experiments of binary classification and multi-classification in the dataset NSL\_KDD, respectively. An intrusion detection method based on data imbalance was suggested by Hu and colleagues [17]. To increase features, strengthen feature variety, and lessen the impact of channel redundancy, personnel suggested an intrusion detection approach based on an adaptive synthetic sampling algorithm and an upgraded convolutional neural network. Based on the model's training and validation against the NSL\_KDD dataset, the effect

accuracy has significantly increased when compared to the conventional model. A convolutional neural network-based model using the convolutional rapid attention method was introduced by Liu [18] et al. to increase the model's accuracy by extracting features. In order to perform intrusion detection, Yao et al. [19] proposed a deep learning model using a convolutional neural network and Transformer. This model reduces the imbalance of the data distribution and invalid features through data enhancement by adaptive synthesis and feature filtering by limiting the gradient of the special province. Impact. The transformer component is then used to explore deeper mapping associations once CNN has constructed a subset of spatial characteristics, increasing the detection accuracy. Therefore, intrusion detection focuses on the present deep learning model. The conventional attention mechanism has been successful in feature extraction, but it is prone to information loss and has low precision. In order to address the aforementioned issues, we created a hybrid attention mechanism in this paper.

### A. DEEP RESIDUAL NETWORKS (DRN)

The generalizability of deep learning models is observed to decline when the convolutional neural network reaches a certain threshold for the number of layers as researchers continue to learn convolutional neural networks in depth. He et al. improved and simplified the CNN and established the deep residual neural network ResNet [20]. The ResNet model is usually composed of multiple residual fast combinations; each residual block contains a convolutional layer (Conv), batch normalization layer (BN), activation function Relu, and shortcut links. The residual block establishes a shortcut link form of implementation to ensure that the features are propagated directly from the bottom to the top layer and the error can be propagated directly backward. Given an input, the output of the first residual block can be expressed as:

$$F(X) + X = f(X) + F(X, W). \quad (1)$$

In the expression, X denotes the shortcut link, the function F denotes the residual block mapping, denotes the residual learning, denotes the network parameters, Relu is the activation function, and in this paper, we use a deep residual network structure consisting of 49 residual blocks combined.

### B. LONG SHORT TERM MEMORY (LSTM)

Hochreiter and Schmidhub [21] put forth the LSTM model. The input gate, output gate, and forgetting gate are three memory units that are combined to create it. The input gate is the information that currently controls the input of this neuron, and the activation function of these three gates is sigmoid. The information that was stored in the neuron at the previous instant is known as the forgetting gate, and the information that the neuron will output at the present instant is known as the output gate. The steps in the computation are listed below:

(1):Oblivion gates  $f_t$  Control the information that the neuron was previously trying to forget [22]:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f). \quad (2)$$

(2): The input gate controls the information that needs to be added and calculates the current moment candidate value  $c'_t$ , where new information needs to be added. The state of the previous neuron  $f_t * C_{t-1}$  and the new candidate information  $i_t C'_t$  are combined to determine the new information by the following equation:

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i). \quad (3)$$

$$C'_t = \tanh(W_c[h_{t-1}, x_t] + b_c) \quad (4)$$

$$C_t = f_t C_{t-1} + i_t C'_t \quad (5)$$

(3): The output gate is to determine how many new cell conditions are  $C_t$  filtered, the tanh function activates neurons  $C_t$  later. Output of the result through the output gate  $O_t$  The formula is as follows:

$$O_t = \sigma(W_o[h_{t-1}, x_t] + b_o). \quad (6)$$

$$h_t = o_t \tanh(C_t). \quad (7)$$

where  $W_f$ ,  $W_i$ ,  $W_c$  and  $W_o$  are the weights of the forgetting gate, the input gate, the update gate, and the output gate, respectively.  $b_f$ ,  $b_i$ ,  $b_c$  and  $b_o$  are the forgetting gate, the input gate, and the update gate, respectively. The output gate calculates the current output  $h_t$  at moment t and  $C_t$  the bias of the updated cell state.

## III. METHODS

This section discusses the methods and algorithms used to categorize attacks used in a networked environment. Unique thermal coding for preprocessing and generation of grayscale images, deep residual networks, and a model based on a combination of hybrid attention algorithms and deep residual networks are described in detail. Fig 1 displays the structure of the model. This paper introduces the hybrid attention mechanism (ESSAM) both before and after the ResNet network. The attention mechanism is introduced before the ResNet network. residual block can screen features beforehand, reduce the amount of information it needs to process, and aid in enhancing computational efficiency. The attention mechanism is added to the model after the residual block, which improves its efficiency and makes it easier to integrate the extracted features. can dynamically modify the weight assigned to certain features, enhancing the model's generalisation capacity and enabling it to respond more effectively to changes in the input data. This helps the model better adapt to changes in the input data and improves its generalisation ability. Intrusion detection is highly temporal. Adding the BiLSTM module to the classification task helps the model capture the temporal information, thereby improving the model's understanding of the data and classification ability.

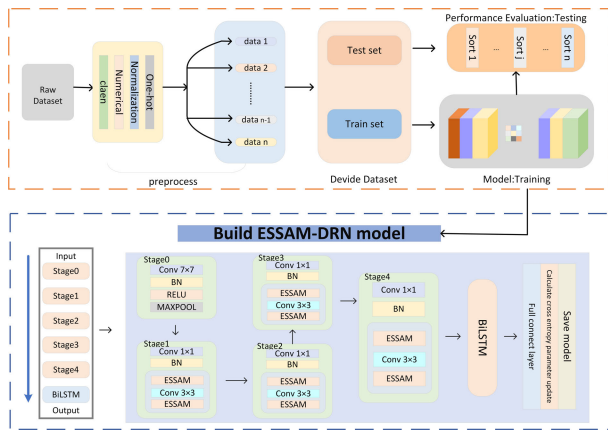


FIGURE 1. Model structure diagram.

**A. DATA PRE-PROCESSING**

Data cleaning, digitization, and standardization are the three basic phases involved in the processing of data collections.

(1) Data cleaning

There are missing feature values and illegal data in the original CICIDS2017 and CICIDS2018 datasets, and data samples with missing features need to be removed when processing the data.

(2) Digitization

The UNSW-NB15 dataset contains three character-type feature types. Because the neural network cannot effectively process character-type data, it is necessary to convert character-type data to numeric type. The three character-type feature types, namely the protocol type, the service type, and the connection state, are each hot-coded and processed as [0,0,1], [0,1,0], and [1,0,0]. The same processing is then applied to other similar attributes.

(3) Standardization

In the sample data, there will be a large numerical difference between different features, which affects the accuracy of the model. After the data is mined, standardization is carried out to eliminate the data differences due to different magnitudes. In this paper, we use the maximum-minimum normalization method to map the values of all the features between [0, 1]. The formula is as follows:

$$X^* = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{8}$$

where  $X^*$  is the normalized eigenvalue,  $X$  is the original eigenvalue,  $X_{\min}$  is the minimum eigenvalue, and  $X_{\max}$  is the maximum eigenvalue. The data is processed to generate a two dimensional gray-scale map. As shown in Fig 2, 3, and 4.

**B. MODEL ARCHITECTURE**

Compared to the traditional convolutional neural network, the increase in the number of convolutional layers leads to a decrease in the generalization ability of the model, so ResNet-50 is used as the backbone of the network, and on top of the backbone network, a bidirectional long- and short-term memory network module and our proposed feature

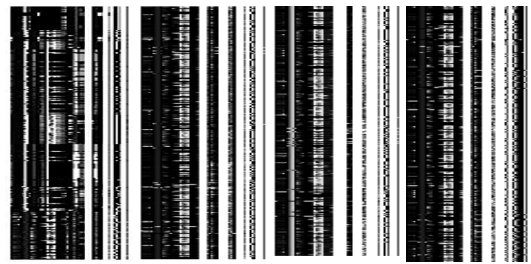


FIGURE 2. UNSW-NB15 processed photo.

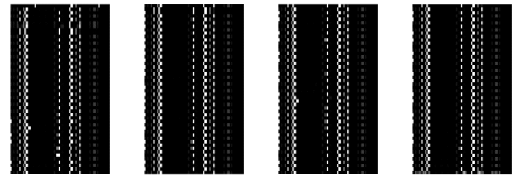


FIGURE 3. CICIDS2017 processed photo.

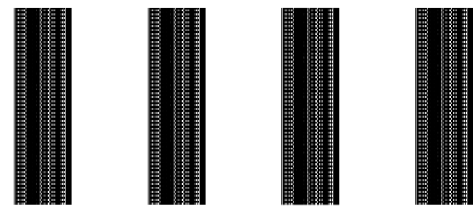


FIGURE 4. CICIDS2018 processed photo.

extraction module under the hybrid channel are added. The hybrid attention module (ESSAM) is added before and after the residual layer of the backbone network to improve the effective extraction of features, while the bi-directional long-short memory network helps to improve the generalization of the model. The hybrid attention mechanism is divided into two parts as follows: As shown in Fig 5.

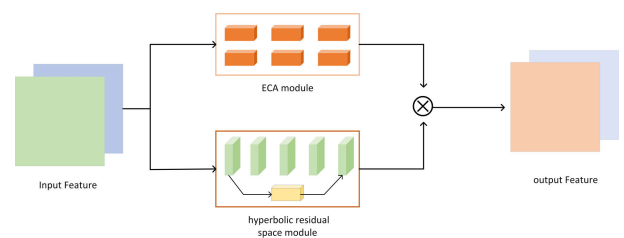


FIGURE 5. Hybrid Attention Module.

1) EFFICIENT CHANNEL ATTENTION MECHANISM (ECA)

The ECA [23] initially performs channel global average pooling (GAP), as seen in Fig 6. The local cross-channel interactions are then captured by ECA using each channel and its  $k$  surrounding channels. Fast one-dimensional convolution is used by ECA to produce channel weights as follows:  $\omega = \sigma(C1D_k(y))$  where  $C1D$  denotes the one-dimensional convolution and  $k$  denotes the kernel size of the one-dimensional convolution. Since the kernel size  $k$  of the one-dimensional convolution is proportional to the channel dimension  $C$ , the



correspondence is defined as follows  $C = \phi(k) = 2^{(y*k-b)}$ . Thus, given the channel dimension  $C$ , the kernel size can be adaptively determined by

$$k = \varphi(C) = \left\lfloor \frac{\log_2(C)}{\gamma} + \frac{b}{\gamma} \right\rfloor_{odd} \quad (9)$$

$\lfloor t \rfloor_{odd}$  where is the closest odd number. In this paper, the parameters of  $\gamma$  and  $b$  are set to 2 and 1, respectively. It is evident from the nonlinear mapping that the high-dimensional channels' interaction range is longer and the low-dimensional channels' interaction range is shorter.

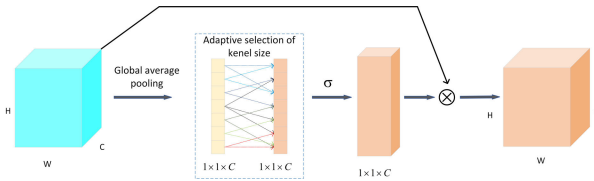


FIGURE 6. ECA Module.

## 2) HYPERBOLIC RESIDUAL SPACE ATTENTION MECHANISMS

As shown in Fig7, The spatial attention is compressed by compressing the channels, and average pooling and maximum pooling are performed in the channel dimension, respectively, with Eqs:

$$\begin{aligned} M_s F &= \sigma(f^{7 \times 7}([AvgPool(F); MaxPool(F)])) \\ &= \sigma(f^{7 \times 7}([F_{avg}^s; F_{max}^s])) \end{aligned} \quad (10)$$

Residual links are introduced at the beginning with the equation:  $res = x \cdot \gamma + (1 - \gamma) \cdot (y - \hat{y})$  where  $x$  is the input feature,  $y$  is the output feature, the predicted output feature,  $\gamma$  is the residual mapping function, and then finally the hyperbolic convolution kernel is used for activation with Eq:

$$g(i, j) = \frac{1}{c} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} f(i+k, j+l), c = N \cdot (i_0 + j_0 + 1) \quad (11)$$

where  $f(i, j)$  is the pixel value in the input image with pixel coordinates  $(i, j)$ .  $g(i, j)$  is the value of the pixel with pixel coordinate  $(i, j)$  in the output image,  $N$  is the size of the convolution kernel,  $i_0, j_0$  is the coordinate of the pixel with pixel coordinate  $(0,0)$  in the output image in the input image and  $C$  is a constant.

## IV. EXPERIMENT

### A. DATA

UNSW-NB 15 dataset: The University of New South Wales published this dataset in 2015. The quantity of characteristics retrieved, the variety of IP addresses utilized for simulation, and the spectrum of attack methods are all greater in the UNSWNB 15 dataset [24]. The dataset comprises a variety

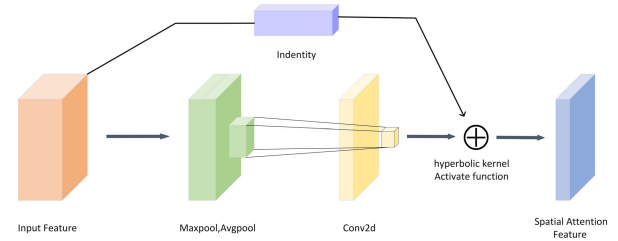


FIGURE 7. hyperbolic residual space module.

### Algorithm 1 hybrid Attention Module

**Input:** Feature map  $F$

**Output:** Attended feature map  $F'$

- 1: EAC Attention:
- 2:  $avg\_pool \leftarrow GlobalAveragePooling(F)$
- 3:  $max\_pool \leftarrow GlobalMaxPooling(F)$
- 4:  $pooling \leftarrow avg\_pool + max\_pool$
- 5:  $fc \leftarrow FullyConnectedLayer(pooling, units = 1, activation = Sigmoid)$
- 6:  $channel\_attention \leftarrow fc \times F$
- 7: Hyperbolic-residual-spatial Attention:
- 8:  $avg\_pool \leftarrow AveragePooling(F, kernel\_size = 7)$
- 9:  $max\_pool \leftarrow MaxPooling(F, kernel\_size = 7)$
- 10:  $concat \leftarrow Concatenate(avg\_pool, max\_pool)$
- 11:  $conv \leftarrow HyperbolicConvolution(pooling, K_h)$
- 12:  $spatial\_attention \leftarrow Sigmoid(conv)$
- 13:  $F' \leftarrow spatial\_attention \times F + F$
- 14: Combine channel and spatial attentions:
- 15:  $F' \leftarrow ECA\_attention + hyperbolic - residual - spatial\_attention$
- 16: **return** Attended feature map  $F'$

### Algorithm 2 Model Workflows

**Inputs:** Training set, test set

**Outputs:** Accuracy, precision, loss rate, F1 score of the model

- Initialize the data
- 2: Input hyperparameters  
Start reading the model
- 4: **for**  $i$  in Epoch **do**  
Extract the data through hybrid attention // as in Algorithm 1
- 6: Input the data into the convolutional layer  
Input the data into deep residual layer
- 8: Train through BILSTM  
**end for**
- 10: Maintain the model  
Validate the model on a test set
- 12: **return** Accuracy, precision, loss rate, F1 score

of sophisticated simulated attacks on network traffic that are both realistic and current. In Table 1, the attack types and data distribution of this dataset are displayed.

The most sophisticated open-source cybersecurity dataset that not only covers the most recent cyberattack scenarios but also satisfies all the requirements for actual cyberattacks is the CICIDS 2017 dataset, which was made available by the Canadian Institute for Cybersecurity Research in 2017 [25]. Both typical traffic and the most prevalent attack traffic currently accessible are included in the CICIDS 2017 dataset, which offers real-world data. To aid in the research of particular assaults, the CICIDS 2017 dataset offers training and test sets divided into categories according to the kind of attack. Each set includes normal traffic and a class of anomalous traffic. Table 2 displays the assault types and data distribution for this dataset.

The CICIDS 2018 [26] dataset has the same characteristics as the 2017 dataset. To properly imitate the assaults, extra gadgets were deployed in the test setting. This dataset was developed using seven distinct attack scenarios, including brute force cracking, heart-bleed attacks, botnet attacks, DoS and DDoS attacks, online attacks, and penetration attacks. Table 3 displays the attack types and data distribution of this dataset.

**TABLE 1. UNSW-NB15 data distribution.**

Category	Count
Normal	93000
Analysis	2677
Backdoor	2329
DoS	16353
Exploit	44525
Fuzzers	24246
Generic	58871
Reconalsance	13987
Shellcode	1511
Worms	174

**TABLE 2. CICIDS-2017 data distribution.**

Category	Count
Normal	529918
Violent Hacking	432074
Backdoor	2329
DoS	440031
Port Scanning	127537
Botnet	189067
Penetration	288566
Web	168186

**TABLE 3. CICIDS-2018 data distribution.**

Category	Count
Benign	2856035
BoT	286191
Brute Force	531
DoS	1289544
Infiltration	93063
SQL Injections	53

## B. EVALUATION INDICATORS

In this paper, Adam is an adaptive learning rate optimisation algorithm that combines momentum and adaptive learning rate. Compared to traditional optimisation algorithms Similar

to stochastic gradient descent (SGD), Adam exhibits faster convergence and superior performance. The model uses Adam as an optimiser to optimise the training. In deep learning, training a model usually requires multiple iterations. This is necessary to allow the model to gradually converge towards an optimal solution. The selection of 100 cycles may serve to regulate training time and computational efficiency. cost while maintaining model performance. The learning rate is an important hyperparameter that controls the step size for updating the model parameters. A smaller learning rate allows the model to converge more stably but may require more iterations to reach the optimal solution, while a larger learning rate speeds up convergence, but it may cause the model to fluctuate or fail to converge during training. We choose a learning rate of 0.001 as the optimal value under the current conditions. problem and model. The hardware and software environments in this paper are as follows: Hardware: AMD Ryzen 9 5900HX with Radeon Graphics 3.30 GHz, 16 GB RAM, GPU: GeForce GTX3070 8 GB; software: Windows 11 64-bit OS; programming language: Python 3; and PyTorch-based deep learning framework. We use four metrics: accuracy (ACC), precision (Pre), recall (Recall), and F1-Score (F1) as evaluation indicators of experimental results, and their formulas are defined as follows:

$$Accuracy(ACC) = \frac{TP + TN}{TP + TN + FP + FN} \quad (12)$$

$$Pre = \frac{TP}{TP + FP} \quad (13)$$

$$Recall = \frac{TP}{TP + FN} \quad (14)$$

$$F_1(F1 - score) = 2 * \frac{Pre * Recall}{Pre + Recall} \quad (15)$$

where TN (True Negative) is the number of predictions with negative results and correct predictions; TP (true positive) is the number of predictions with positive results and correct predictions; FP (false negative) is the number of predictions with negative results and incorrect predictions; and FP (false Positive) is the number of predictions with positive results and incorrect predictions.

## C. EXPERIMENTAL RESULTS

### 1) RESULTS OF BICLASSIFICATION

Four experiments—code-named 1, 2, 3, and 4—are designed in this paper to accurately verify that each model module has an enhancement effect on the model. No. 1 shows the network structure that is left over after the proposed hybrid attention mechanism and BILSTM module are added. While No. 3 only has the attention module and lacks the BILSTM module, No. 2 only has the BILSTM module and no hybrid attention mechanism. BILSTM module number 4 represents the original network architecture. The validation is carried out independently for each of the three datasets, and the outcomes are displayed in the following Fig. 8. The comparative tests above make it clear that our novel hybrid attention is useful in improving intrusion detection accuracy. The aforementioned

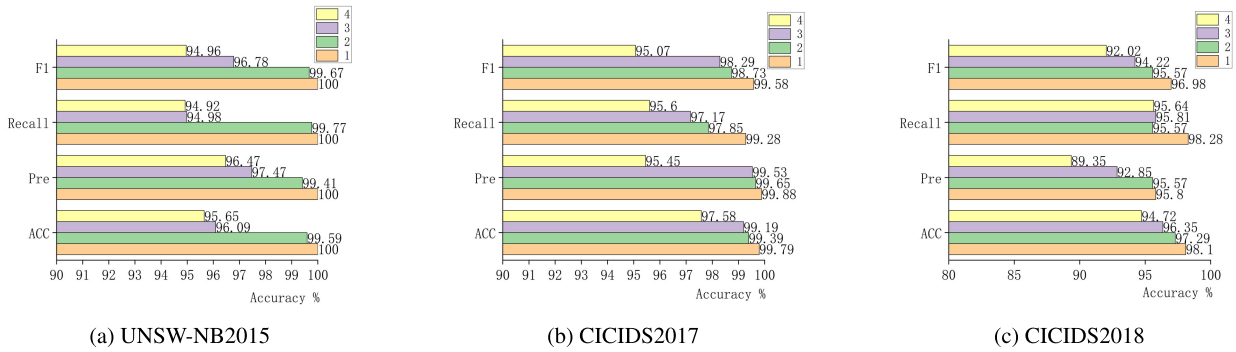


FIGURE 8. Comparison of results.

figures demonstrate how the addition of the new hybrid attention mechanism greatly increased the model’s accuracy; Through the above ablation experiments, it is demonstrated that the hybrid attention module proposed in this paper improves the ability to capture and learn effective features. The integration of the BiLSTM module for memorization in the temporal feature dimension enhances accuracy. In the binary classification experiments, The accuracy rates of 100%, 99.70% and 98.10% were achieved on the UNSW-NB15, CICIDS2017, and CICIDS2018 datasets, respectively, which indicates that the model has a better ability to determine cyberattacks and normal traffic.

2) MULTI-CLASSIFICATION RESULTS

a: RESULTS OF EACH DATASET

In this thesis use three datasets to validate the performance of the model: UNSW-NB2015, which contains 9 types of attacks and 1 type of normal situation; CICIDS2017, which contains 7 types of attacks and 1 type of normal situation; and CICIDS2018, which contains 6 types of attacks and 1 type of normal situation. The results are shown in Fig 9.

The dataset was subjected to multi-class detection experiments, in which the accuracy was 96.37% on the UNSW-NB15 dataset, 98.12% on the CICIDS2017 dataset, and 99.06% on the CICIDS2018 dataset, and it can be seen in Fig. 9 that it also demonstrated excellent detection ability on the UNSW-NB15 dataset, with assorted accuracies. are more than 83%. In dataset CICIDS-2017 and dataset CICIDS-2018, the accuracy of all categories exceeds 85%. We apply the hybrid attention module and BiLSTM to residual data. Fig. 10 shows that networks of various depths produced good results on the residual network with a depth of 50, leading us to select ResNet50 as the the network backbone of the model.

b: MODEL COMPARISON

In the experiments of this paper, we compare them with some recent related models. In the experiments, we use the same dataset to compare the model performance of each case. The experimental results are shown in Table 4.

Through the results we can get that our model is better than the recent models in all the metrics, in the dataset UNSW-NB15, the best model is BiLSTM proposed by Ganesh B with

TABLE 4. Comparison with recent models.

Method	Dataset	ACC %	Pre %	Recall %	F1 %
Random forest [27]	UNSW-NB15	89.9	94.6		91.87
DNN [28]	UNSW-NB15	83.8	83.59	83.80	83.77
SMO-HPSO [29]	UNSW-NB15	94.19	93.32	94.12	99.18
AAFSA AND GA-GR [30]	UNSW-NB15	94.48	94.29	94.56	94.42
BILSTM [31]	UNSW-NB15	95	95	95	94
SVM [32]	CICIDS-2017	78.4	99.16	75.21	76.66
DNN [33]	CICIDS-2017	96.2	92	96.2	96.5
Random forest [34]	CICIDS-2017		98.50	92.30	95.30
CNN-PCC [35]	CICIDS-2017	97	87	96	73
EFS-SMOTE-AdaBoost [36]	CICIDS-2017	91.47	81.69	95.76	88.17
Decision tree [37]	CICIDS-2018	92.8	92.8	92.81	92.81
DNN [38]	CICIDS-2018	98.5	98.41	98.31	98.55
CU-BILSTM [39]	CICIDS-2018	98.9	98.64	98.71	98.82
CNN [38]	CICIDS-2018	98.98	98.47	98.94	98.86
HFS+LightGBM [40]	CICIDS-2018	97.72	99.33	96.06	97.57
<b>Propose model</b>	<b>UNSW-NB15</b>	<b>96.37</b>	<b>95.03</b>	<b>95.19</b>	<b>95.02</b>
	<b>CICIDS-2017</b>	<b>98.12</b>	<b>98.52</b>	<b>98.33</b>	<b>98.34</b>
	<b>CICIDS-2018</b>	<b>99.06</b>	<b>99.31</b>	<b>99.28</b>	<b>99.28</b>

95% accuracy followed by Genetic Algorithm based neural network model proposed by Anushiya R et al. with 94.48% accuracy, whereas the accuracy of our proposed model is 96.37% and F1 score is also better than the model, in the dataset CICIDS2017, the best model is the intrusion detection model based on the combination of CNN and PCC proposed by Bhavsar M et al. and its accuracy is at 97%, followed by the DNN model architecture proposed by Muthanna and

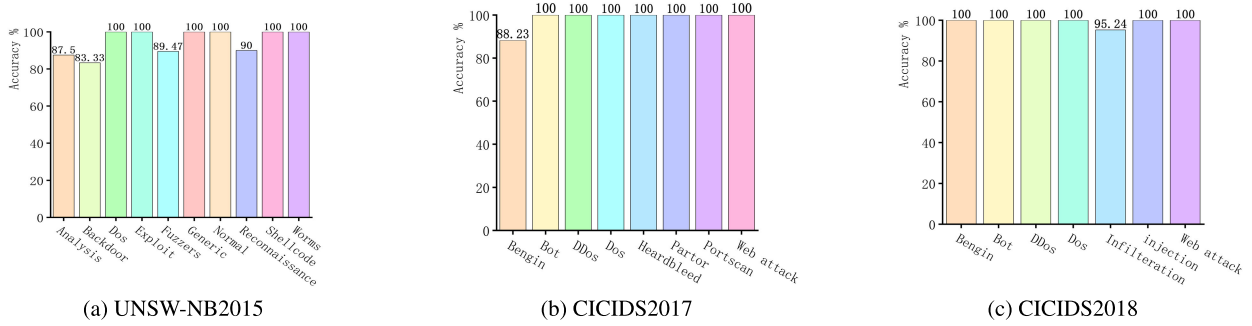


FIGURE 9. results of various attacks.

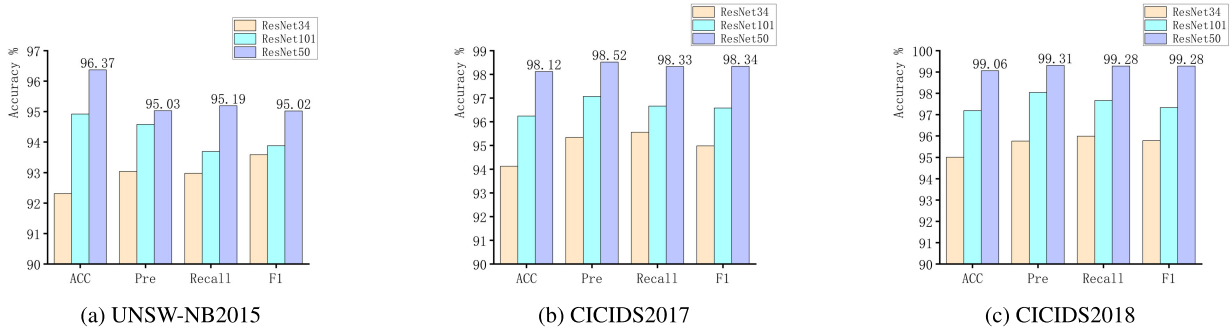


FIGURE 10. Residual network results for different depths.

its accuracy above reaches to 96.2, whereas, our model in the CICIDS2017 dataset can reach 98.59% and is higher than other models on CICIDS2018 dataset. The experimental results show that our proposed model achieves good results on all three datasets.

In this paper, experiments are conducted on UNSW-NB15, CICIDS-2017, and the CICIDS-2018 dataset.

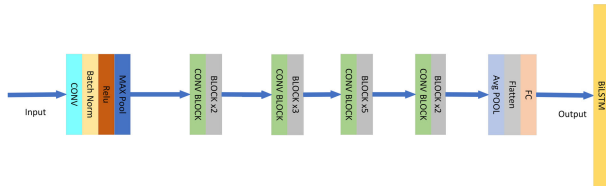


FIGURE 11. Structure after removing the Attention module.

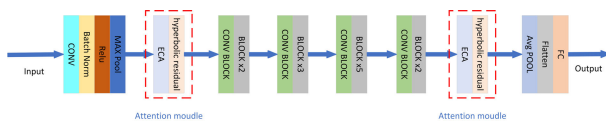


FIGURE 12. Structure after removing the BILSTM module.

c: ABLATION EXPERIMENTS

The method proposed in this paper contains two main factors: a hybrid attention module and a bidirectional long and short memory module. In order to verify whether these two modules are effective on multicategorization as well as to verify whether our hybrid attention mechanism is superior to the Convolutional Attention Mechanism (CBAM), The hybrid attention module, long and short memory network module, and attention mechanism will be removed, respectively, and the model is shown in Fig 11, 12, 13, and 14.

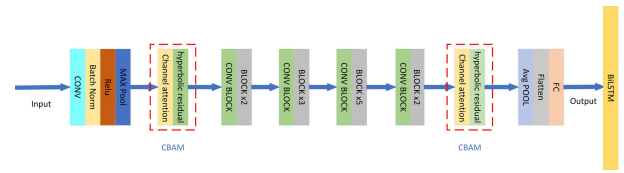


FIGURE 13. Structure after switching Attention to CBAM.

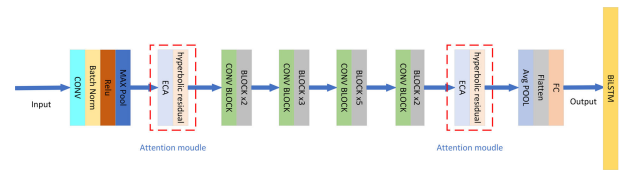


FIGURE 14. Architecture of this paper.

I) LONG AND SHORT MEMORY NETWORK MODULE

The long and short memory modules are able to capture the semantic relationships of long-distance contexts, and are able to memorize and classify the input features well. In our experiments, we remove this module to verify the effectiveness of this module in the model.

II) HYBRID ATTENTION MODULE

The hybrid attention module extracts the desired information more accurately and improves the accuracy of the input information and the accuracy of the model by extracting



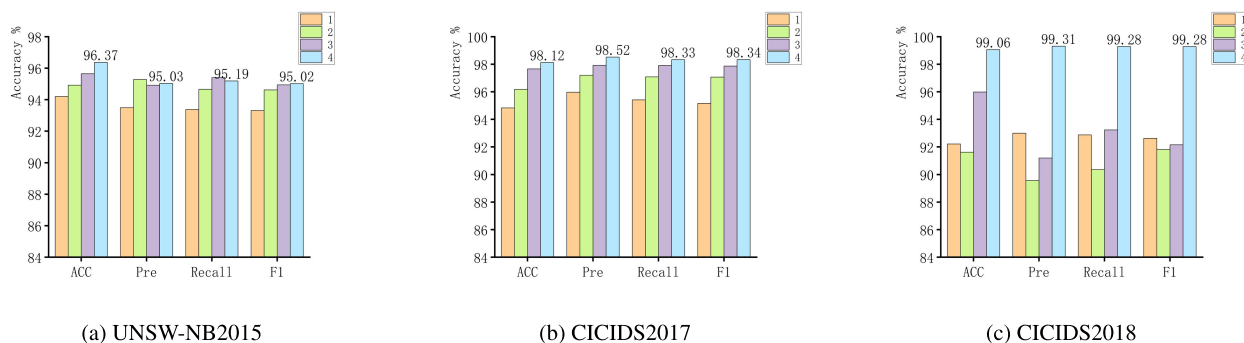


FIGURE 15. Results of ablation experiments.

the feature information of the channel assessment space. Therefore, we replace it with the CBAM attention module to verify the effectiveness of this module compared to CBAM attention for enhancement in the network.

The experiments use the numbers 1, 2, 3, and 4 to represent the no-attention mechanism join, CBAM attention module, no-BiLSTM module, and the model of this paper, respectively. The results are analyzed and shown in Figure 15. From the experimental results, it can be found that the results of the model in this paper, in which lab 4, After replacing the hybrid attention module and removing the long and short memory network module, the accuracy has decreased by 2-7%, and removing any of the modules on the backbone model has a not insignificant effect on its accuracy. Our proposed hybrid attention mechanism leads in accuracy and F1 score compared to the convolutional attention mechanism, reflecting the superiority of our proposed attention over the CBAM on the three datasets and the improved generalization ability of the model.

## V. CONCLUSION

In this thesis, we propose a new attention mechanism acting on top of the residual network, which integrates spatial and temporal features, fully combines the structure and characteristics of network attacks, and has the characteristics of being more efficient and accurate in terms of channel, optimizing the performance compared with the previous CBAM attention mechanism, combining with the BiLSTM module, which is more accurate in terms of temporal information and more accurate in terms of the classification of the model, which improves the efficiency of the model. Validation with three datasets shows that our proposed method enhances the accuracy of the model and improves its generalization ability. Future main research directions:

1. In order to further improve the accuracy of the model, we will continue to conduct in-depth research on feature engineering, and we will use different feature extractors and loss functions to narrow down the range of features so that the model can be more accurate.

2. One of the ways to explain the inner workings of the neural network model is the mechanism of attention, which analyzes the importance of the input and output information

by calculating the attention. So, our proposed module can also make an impact on explainable machine learning. The research on the attention mechanism will be continued in depth.

## ACKNOWLEDGMENT

The authors would like to sincerely thank the teachers for their ideas and assistance during the experiments.

## REFERENCES

- [1] K. Raghavan, M. Desai, and P. V. Rajkumar, "Multi-step operations strategic framework for ransomware protection," *SAM Adv. Manage. J.*, vol. 85, no. 4, pp. 2–16, 2020.
- [2] P. V. Rajkumar, K. Raghavan, and M. Desai, "Cyber security and hybrid work environments," *SAM Adv. Manage. J.*, vol. 88, no. 3, pp. 44–56, 2023.
- [3] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3242–3254, Mar. 2021.
- [4] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101863.
- [5] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical network," *IEEE Access*, vol. 8, pp. 32464–32476, 2020.
- [6] K. Zheng, Z. Cai, X. Zhang, Z. Wang, and B. Yang, "Algorithms to speedup pattern matching for network intrusion detection systems," *Comput. Commun.*, vol. 62, pp. 47–58, May 2015.
- [7] D. Papamartzivanos, F. G. Marmol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019.
- [8] J.-J. Fu and X.-L. Zhang, "Gradient importance enhancement based feature fusion intrusion detection technique," *Comput. Netw.*, vol. 214, Sep. 2022, Art. no. 109180.
- [9] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: A survey," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102177.
- [10] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and bot-IoT attacks traffic identification for Internet of Things in smart city," *Future Gener. Comput. Syst.*, vol. 107, pp. 433–442, Jun. 2020.
- [11] P. V. Rajkumar and R. Sandhu, "Safety decidability for pre-authorization usage control with identifier attribute domains," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 3, pp. 465–478, May 2020.
- [12] P. V. Rajkumar and R. Sandhu, "Safety decidability for pre-authorization usage control with finite attribute domains," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 5, pp. 582–590, Sep. 2016.
- [13] M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique," *J. Netw. Comput. Appl.*, vol. 191, Oct. 2021, Art. no. 103160.

- [14] J. Sinha and M. Manollas, "Efficient deep CNN-BiLSTM model for network intrusion detection," in *Proc. 3rd Int. Conf. Artif. Intell. Pattern Recognit.*, Jun. 2020, pp. 223–231.
- [15] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Future Gener. Comput. Syst.*, vol. 113, pp. 418–427, Dec. 2020.
- [16] B. Gan, Y. Chen, Q. Dong, J. Guo, and R. Wang, "A convolutional neural network intrusion detection method based on data imbalance," *J. Supercomput.*, vol. 78, no. 18, pp. 19401–19434, Dec. 2022.
- [17] Z. Hu, L. Wang, L. Qi, Y. Li, and W. Yang, "A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network," *IEEE Access*, vol. 8, pp. 195741–195751, 2020.
- [18] Y. Liu, J. Kang, Y. Li, and B. Ji, "A network intrusion detection method based on CNN and CBAM," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.
- [19] R. Yao, N. Wang, P. Chen, D. Ma, and X. Sheng, "A CNN-transformer hybrid approach for an intrusion detection system in advanced metering infrastructure," *Multimedia Tools Appl.*, vol. 82, no. 13, pp. 19463–19486, May 2023.
- [20] K. He, X. Zhang, S. Ren, and J. Sun, "Identity mappings in deep residual networks," in *Proc. Eur. Conf. Comput. Vis.* Cham, Switzerland: Springer, 2016, pp. 630–645.
- [21] S. Hochreiter and J. Schmidhuber, "LSTM can solve hard long time lag problems," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 9, 1996, pp. 1–11.
- [22] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Syst. Appl.*, vol. 185, Dec. 2021, Art. no. 115524.
- [23] Q. Wang, B. Wu, P. Zhu, P. Li, W. Zuo, and Q. Hu, "ECA-Net: Efficient channel attention for deep convolutional neural networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2020, pp. 11531–11539.
- [24] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.
- [25] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 479–482, 2018.
- [26] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Proc. Comput. Sci.*, vol. 167, pp. 636–645, Jan. 2020.
- [27] S.-J. Wang, C. X. Cai, Y.-W. Tseng, and K. S. Li, "Feature selection for malicious traffic detection with machine learning," in *Proc. Int. Comput. Symp. (ICS)*, Dec. 2020, pp. 414–419.
- [28] Y. Zhang, Y. Gandhi, Z. Li, and Z. Xiao, "Improving the classification effectiveness of network intrusion detection using ensemble machine learning techniques and deep neural networks," in *Proc. Int. Conf. Intell. Data Sci. Technol. Appl. (IDSTA)*, Sep. 2022, pp. 117–123.
- [29] S. Ethala and A. Kumarappan, "A hybrid spider monkey and hierarchical particle swarm optimization approach for intrusion detection on Internet of Things," *Sensors*, vol. 22, no. 21, p. 8566, Nov. 2022.
- [30] R. Anushiya and V. S. Lavanya, "A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of Things," *Meas., Sensors*, vol. 26, Apr. 2023, Art. no. 100700.
- [31] B. Ganesh and S. Sridevi, "Analysis of hybrid deep learning models for efficient intrusion detection," in *Proc. Int. Conf. Netw. Commun. (ICNWC)*, Apr. 2023, pp. 1–6.
- [32] A. Yulianto, P. Sukarno, and N. A. Suwastika, "Improving AdaBoost-based intrusion detection system (IDS) performance on CIC IDS 2017 dataset," *J. Phys., Conf. Ser.*, vol. 1192, Mar. 2019, Art. no. 012018.
- [33] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.
- [34] Z. Chen, L. Zhou, and W. Yu, "ADASYN-random forest based intrusion detection model," in *Proc. 4th Int. Conf. Signal Process. Mach. Learn.*, 2021, pp. 152–159.
- [35] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021.
- [36] S. Sivamohan, S. S. Sridhar, and S. Krishnaveni, "An effective recurrent neural network (RNN) based intrusion detection via bi-directional long short-term memory," in *Proc. Int. Conf. Intell. Technol. (CONIT)*, Jun. 2021, pp. 1–5.
- [37] A. Singh, J. Prakash, and G. Kumar, "Intrusion detection system: A comparative study of machine learning-based IDS," *Tech. Rep.*, 2022.
- [38] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE," *IEEE Access*, vol. 11, pp. 37131–37148, 2023.
- [39] M. S. A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq, and W. A. M. Abdullah, "Towards SDN-enabled, intelligent intrusion detection system for Internet of Things (IoT)," *IEEE Access*, vol. 10, pp. 22756–22768, 2022.
- [40] S. Seth, G. Singh, and K. Kaur Chahal, "A novel time efficient learning-based approach for smart intrusion detection system," *J. Big Data*, vol. 8, no. 1, pp. 1–28, Dec. 2021.



**XUNTAO HU** is currently pursuing the M.S. degree with Anhui University of Science and Technology. His current research interests include deep learning and information security.



**XIANCAI MENG** was born in January 1991. He received the Ph.D. degree. Since September 2020, he has been with the Neutron Technology Application Center of Energy Research Institute, Hefei Comprehensive National Science Center (Energy Laboratory of Anhui Province). He is currently the Deputy Head of the Research Group of Neutron Beam Technology. He is an Associate Researcher and the Master's Tutor. His research interests include compatibility of fusion reactor materials with liquid lithium and lithium alloys and neutron beam technology. His scientific research presided over or participated in the National Natural Science Foundation of China, the Ministry of Science and Technology Key Research and Development special projects, and other national enterprises and universities and other cooperative research projects more than ten.



**SHAOQING LIU** was born in Shushan District, Hefei, Anhui, China, in 1991. He received the Ph.D. degree in computer application technology from the University of Science and Technology of China, Hefei, in 2022. He is currently a Research Assistant with the Institute of Energy, Hefei Comprehensive National Science Center. His research interests include the development of rotating machinery fault diagnosis, predictive maintenance, and deep transfer learning.



**LIZHEN LIANG** was born in 1984. He received the degree in physics from Shandong Jianzhu University, in 2006, and the M.S. and Ph.D. degrees from the Institute of Plasma Physics, Chinese Academy of Sciences. He was a Visiting Scholar with the National Institute for Fusion Science on LHD, Japan, in 2019. He is currently an Associate Professor. His research interests include beam transmission, spectral diagnosis, and neutral beam physical experiments. His research currently emphasis focuses on design of NNBI and optical emission spectrum for negative ion based neutral beam injection. He has participated in the development work of developing 4MW beamline for EAST.

...