frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 12 September 2025
DOI 10.3389/fphy.2025.1616779

OPEN ACCESS

EDITED BY
Stefano Rinaldi,
University of Brescia, Italy

REVIEWED BY
Neeraj Kumar Pandey,
Graphic Era University, India
Yue Zhang,
Nanjing Agricultural University, China

*CORRESPONDENCE
Chenxi Zhu,
32023050126@cueb.edu.cn

RECEIVED 23 April 2025
ACCEPTED 25 August 2025
PUBLISHED 12 September 2025

CITATION
Zhu C and Li Z (2025) An agricultural network security situation awareness method based on fusion model in digital economy.
Front. Phys. 13:1616779.
doi: 10.3389/fphy.2025.1616779

An agricultural network security situation awareness method based on fusion model in digital economy

Chenxi Zhu[1]* and Zhixian Li[2]

[1]School of labor Economics, Capital University of Economics and Business, Beijing, China, [2]School of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang, China

Nowadays, the digital transformation of agriculture puts forward higher requirements for network security. In response to the complex network traffic data and chaotic attack data cycles in the current agricultural network environment, it is difficult for the network security situation awareness methods to effectively extract network security situation elements and perceive network security status. Therefore, this paper proposes a fusion model-based agricultural network security situation awareness method, namely, MSCNN-ResNeXt-Transformer. Firstly, ResNeXt is improved by fusion model, using Multi-Scale Convolutional Neural Network (MSCNN) instead of a single scale convolution structure. This enables the agricultural network security situation awareness model in digital economy to comprehensively extract network security situational elements from multiple scales. The Efficient Channel Attention (ECA) mechanism is then employed to further refine and characterize the data processed by the improved ResNeXt. Finally, the Transformer is used to optimize the proposed model and improve the accuracy of agricultural network security situation awareness in digital economy. The experimental results show that the accuracy, recall and F1 of MSCNN-ResNeXt-Transformer on MOORE, KDDCUP99 and WSN-DS are significantly better than traditional models, providing effective technical support for agricultural digital security protection.

KEYWORDS

security situation awareness, fusion model, transformer, agricultural network security, digital economy

1 Introduction

In digital economy and the deepening of agricultural digital transformation, the issue of agricultural network security is becoming increasingly prominent. Smart agriculture relies on emerging technologies such as the Internet of Things (IoT), which not only improve agricultural production efficiency but also bring unprecedented cybersecurity risks [1]. The digital economy becomes an important engine for global economic growth and agriculture, as the fundamental industry of the national economy, is accelerating its development towards digitization and intelligence.

Agriculture is deeply integrated into the development process of the digital economy. The digital transformation of agriculture aims to use modern information technology to transform and upgrade the entire industry chain, including agricultural production, operation, management and services. In the agricultural production process, precision agriculture technology is flourishing. Through technologies such as satellite positioning, sensors and drones, farmers can monitor soil conditions and meteorological changes in real time, significantly improving agricultural production efficiency, reducing resource waste. In terms of agricultural management and services, digital technology helps government departments achieve refined management of agricultural resources, agricultural production processes and agricultural product safety. By establishing an agricultural big data platform, integrating various agricultural information resources, providing scientific basis for agricultural disaster warning and agricultural technology promotion.

With the continuous deepening of digitalization in agriculture, the dependence on network information technology in the agricultural field is increasing, which also makes the network security risks faced by agriculture growing day by day. Attackers may infiltrate devices such as IoT, tamper with sensor data and make agricultural production decisions incorrectly. Agricultural e-commerce platforms and agricultural product trading systems also face many cybersecurity threats. Security incidents such as phishing, malware attacks and data breaches occur from time to time [2, 3]. Once the user information and transaction data of e-commerce platforms are leaked, it not only harms the rights and interests of consumers, but also seriously damages the reputation of agricultural enterprises. The agricultural big data platform gathers massive amounts of agricultural production, market and other data, which have extremely high value. However, its security also faces serious challenges, as attackers may obtain or tamper with data through network infiltration, internal personnel violations and other means, affecting the scientific nature of agricultural policy formulation and the effectiveness of agricultural management.

The agricultural network environment has significant particularities, with diverse data sources and complex structures, including traditional network traffic data, as well as environmental monitoring data collected by various agricultural sensors, crop growth data, etc. These data have significant differences in time scale, spatial dimension, and semantic features, which pose great difficulties for data fusion and analysis. Secondly, agricultural production has obvious seasonal and timeliness characteristics, which requires safety monitoring systems to have real-time response capabilities. However, traditional rule-based safety analysis methods often suffer from detection lag. Furthermore, with the continuous evolution of attack techniques, the attack methods against agricultural systems become increasingly complex and covert. From early simple scanning and detection to advanced threats such as APT attacks and 0 day vulnerability exploitation, this raises higher requirements for security detection technology [4–6]. In addition, the resource limited nature of agricultural field equipment is also an important constraint factor. Many agricultural IoT nodes limite computing power and insufficient storage space, making it difficult to deploy complex security methods.

Faced with increasingly complex agricultural cybersecurity threats, traditional cybersecurity protection methods are gradually exposing their limitations. Traditional firewall technology is mainly based on pre-set rules to control network traffic and prevent unauthorized external access. However, in the agricultural IoT environment, there are numerous types of devices, complex communication protocols and constantly emerging new network attack methods, making it difficult for firewalls to respond to unknown attack behaviors. Intrusion detection system (IDS) and intrusion prevention system (IPS) detect and defend against attacks by monitoring abnormal behavior in network traffic [7]. However, in the agricultural network environment, due to the complexity and variability of normal business traffic patterns, false positives and false negatives are prone to occur. Although encryption technology can ensure the confidentiality of data during transmission and storage, traditional security measures are difficult to effectively analyze and detect the content of encrypted data. In the application scenario of agricultural big data, a large amount of encrypted data cannot be timely discovered for potential hidden security risks during sharing and use. In addition, traditional agricultural network security protection measures often operate independently and lack effective collaboration and linkage mechanisms. Security devices such as firewalls and encryption systems cannot share information in real time, making it difficult to form an overall security protection force. When facing complex multi-stage and distributed network attacks, it is difficult to provide timely and comprehensive defense and response.

Network security situation awareness aims to collect and analyze various security related information in the network, conduct real-time assessment and prediction of network security status and provide a basis for timely and effective security protection measures. The fusion model based on deep learning can integrate heterogeneous data from multiple sources, improving the accuracy and comprehensiveness of situational awareness. There is a large amount of data from different devices, systems and applications in the agricultural network environment, such as operational data of IoT devices, network traffic data, etc. A single data source is difficult to fully reflect the network security situation. The fusion model based on deep learning can fuse and process these multi-source heterogeneous data, mine potential correlations between data, more accurately identify network attack behaviors and evaluate network security risks [8]. Faced with the constantly emerging new network attack methods, fusion model based on deep learning can quickly adjust their learning strategies and update their ability to recognize attack behaviors in a timely manner. By using fusion model to analyze historical and real-time data, it is also possible to predict the network security situation in the future, warn potential security threats in advance and provide forward-looking support for security decisions.

In summary, against the backdrop of the booming development of the digital economy and the promotion of agricultural digital transformation, agricultural network security is facing unprecedented challenges. The agricultural network security situation awareness method based on fusion model can more comprehensively perceive the agricultural network security situation by integrating multi-source data and leveraging the advantages of multiple methods, providing strong technical support for ensuring the smooth progress of agricultural digitalization process [9]. Our main contributions are summarized as follows.

1. In response to the difficulty of extracting network security situation elements in agricultural environment under digital economy, this paper proposes MSCNN-ResNeXt-Transformer. It improves ResNeXt by integrating MSCNN instead of single scale convolution to achieve comprehensive extraction of network security situation elements from multiple perspectives, scales and directions.
2. MSCNN-ResNeXt-Transformer incorporates ECA mechanism to weight ResNeXt, leverages the Transformer encoder to optimize the model network, thereby enhancing the accuracy of agricultural network security situation awareness in digital economy.
3. Multiple experiments are conducted on diverse datasets, with comparisons against advanced baselines, to validate the effectiveness of MSCNN-ResNeXt-Transformer.

The rest of this paper consists of four parts. Section II; is related literature. Section III provides a detailed introduction to the research on the fusion model of agricultural network security situation awareness driven by deep learning in digital economy. Section IV analyzes the comparative effect and performance of the proposed MSCNN-ResNeXt-Transformer through experiments and metrics. Finally, Section V is the summary.

2 Literature review

In terms of traditional research methods, [10] established a Bayesian network-based situational assessment model for experimental unmanned aerial vehicles (UAVs). To address the problem of difficulty in obtaining Bayesian network parameters, they proposed an improved whale optimization algorithm (WOA) based on prior parameter intervals (IWOA-PPI) for parameter learning. The experimental results indicated that IWOA-PPI was highly effective. The correctness and feasibility of the proposed method had also been demonstrated in scenario experiments. [11] proposed MAVIDS, which used single class classifiers such as autoencoders and principal component analysis (PCA), OCSVM and LOF to detect abnormal situations. Using flight records as training data was a multifunctional method. [12] proposed an intrusion detection system (IDS) for detecting flight anomalies and network attacks in drone swarms, which applied both unsupervised and supervised machine learning methods. In unsupervised methods, stacked autoencoders and federated learning were used to detect abnormal situations during flight. Supervised algorithms, such as LightGBM, were used to identify denial of service (DoS) attacks on drone networks and used generative adversarial networks (GANs) for data balancing. The results obtained by IDS were promising, indicating the effectiveness of the selected techniques, especially federated learning. This utilized the distribution characteristics of drone populations and ensured data privacy. [13] proposed a joint continuous learning framework based on Digital Twin Network (DTN), which used stacked broad learning system (SBLS) for fast continuous learning and training of IDS models. For improving the efficiency and quality of training and aggregation processes, an asynchronous federated learning architecture was adopted. And a drone selection scheme based on deep deterministic policy gradient (DDPG) assisted DTN was proposed to assist in the aggregation of global IDS. The algorithm was validated using the CIC-IDS2017, simulation results showed that it achieved higher efficiency than existing federated learning schemes, but was not validated using wireless datasets.

Deep learning, relying on its excellent generalization and self-learning abilities, had been widely applied by scholars and experts in the areaof network security situation awareness [14, 15]. [16] proposed a novel model based on the parsimonious memory unit (PMU), namely, bidirectional parsimonious memory unit (BIPMU), to address the low accuracy of network security situation assessment caused by the large capacity, diversity and high latitude characteristics of wireless network data. Compared to PMU, BIPMU's advantage lied in its bidirectional temporal modeling capability. This model integrated forward and backward propagation paths, which not only effectively captured short-term dynamic features, but also deeply explores long-term operating patterns. The experimental results showed that the method adopted had made breakthroughs in efficiency and accuracy. [17] proposed a data-driven WNN-M prediction model that combined MODWT method and hybrid WNN architecture to improve the accuracy of long-term predictions. The experimental results showed that compared with the traditional WNN, WNN-M reduced the root mean square error (RMSE) by 19.87% and the absolute RMSE by 4.05%. [18] proposed a network security situation prediction model based on Time Convolutional Network (TCN) and Transformer to solve the long-term prediction problem of time series. [19] proposed a network security situation assessment method based on network attack behavior classification to solve the problems of difficult feature extraction and poor timeliness in existing network security situation assessment methods. A network attack behavior classification model had been designed, which combined the characteristics and advantages of parallel feature extraction network (PFEN), bidirectional gated recurrent unit (BiGRU) and attention mechanism to extract key data from different network attack behaviors. The experimental results showed that compared with traditional methods, the accuracy of the network attack behavior classification model had increased by 5.28% and the recall rate has increased by 5.65%, proving the effectiveness of the proposed method. [20] proposed a distributed framework based on Long Short Term Memory (LSTM) for detecting intrusions in unmanned aerial vehicles. This framework deployed the recurrent neural network (RNN) within each drone and each drone independently performed detection work for its own attack situation. At the same time, the centralized LSTM-RNN set up on the base station verified the attack situation, made the final judgment and informed other drones of the results.

3 Deep learning oriented agricultural network security situation awareness in digital economy

3.1 Overview of MSCNN-ResNeXt-transformer

Multi channel RNN increases the number of parallel paths for feature processing by introducing cardinality. Each path can undergo independent transformations, which can increase the

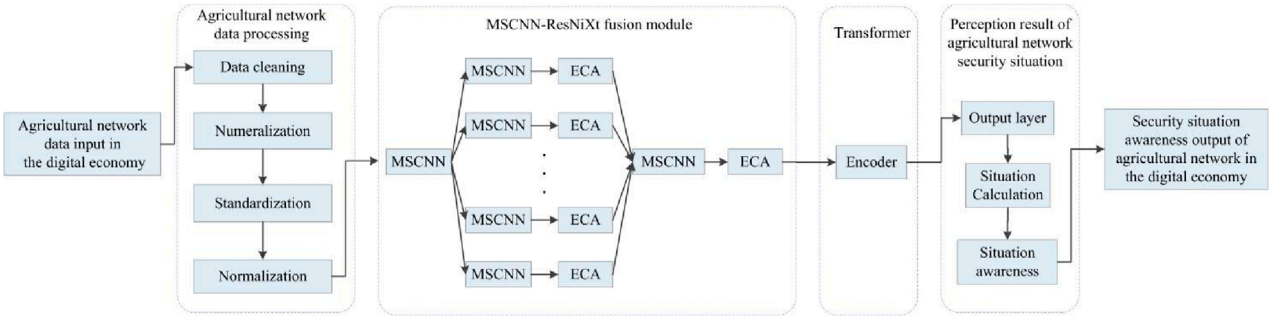

FIGURE 1
Agricultural network security situation awareness in digital economy based on MSCNN-ResNeXt-Transformer.

nonlinear and representational capabilities of the model, enabling it to learn rich and representative features. Multi channel RNN utilizes splitting, transformation and merging strategies in a simple and scalable manner to improve model complexity and expressiveness without increasing the number of parameters. However, the multi channel RNN has a single convolution scale and cannot extract data features from multiple directions, angles and scales. Therefore, this paper proposes MSCNN-ResNeXt-Transformer, which uses a fusion structure of MSCNN instead of a single scale convolution structure to enhance the feature extraction capability of agricultural network in digital economy.

This paper first uses data preprocessing techniques to process the dataset, including data cleaning, numerization, standardization and normalization. Then, the preprocessed agricultural network data in digital economy is input into the MSCNN-ResNeXt fusion module. It uses a MSCNN structure instead of a single scale convolution structure to extract features from the input agricultural network data in digital economy, for achieving the goal of extracting network security situation elements from multiple perspectives, scales and directions. The data processed by the MSCNN-ResNeXt fusion module is then weighted by ECA to improve its feature expression ability. Transformer is utilized to optimize the MSCNN-ResNeXt fusion module to improve the accuracy of network security situation awareness. Finally, the situation value that fully represents the current network security situation is calculated and output through situation value calculation. The schematic diagram based on MSCNN-ResNeXt-Transformer is shown in Figure 1.

The convolutional layer of each residual block in ResNeXt is divided into multiple branches, each with the same structure and independent parameter learning, which can increase the width of the model and improve the diversity of agricultural network security situation features in digital economy. The same branch structure enables MSCNN-ResNeXt-Transformer to have good scalability. But it also limits the scale and perspective of the model's extraction of agricultural network data security features in digital economy, making it unable to extract data features more effectively from multiple perspectives and angles. Therefore, by improving ResNeXt and integrating model structures, MSCNN constructs a model more suitable for agricultural network security situation awareness in the digital economy. For improving the accuracy of agricultural network security situation awareness in digital economy, the encoder of Transformer is also used to optimize the model structure, which can comprehensively perceive the security situation of the network.

3.2 MSCNN-ResNeXt fusion module

ResNeXt is a simple, highly modular network architecture proposed by the University of California, San Diego and the Facebook Ai Research team for image classification. ResNeXt has scalability and modules have the same topology structure [21]. ResNeXt is an upgraded version based on ResNet, with the main goal of improving the model's expressive and generalization abilities, thereby enabling better extraction of agricultural network data features in digital economy and enhancing the model's results. ResNeXt introduces a new concept called Cardinality. Cardinality refers to the number of parallel paths used for feature processing in a network and can also be understood as the topological structure between multiple subnetworks. This idea is similar to combining multiple smaller sub networks to form a larger network.

In ResNeXt, each branch of the residual block is divided into multiple paths and each path is independently transformed. This increases the non-linear and representational capabilities of the model, allowing the network to learn more diverse characteristics of agricultural network security in digital economy. Meanwhile, by increasing the cardinality, ResNeXt can improve the complexity and expressiveness of the model without increasing the number of parameters. ResNeXt inherits ResNet's repetition strategy but increases the number of paths. The modules in ResNeXt perform a set of transformations, each performed in a low dimensional embedding, summarized through summation and each path has the same topology. This design makes ResNeXt scalable to any number of conversions. During the construction process of ResNeXt, the cardinality can be adjusted according to requirements. This allows for flexible design of the network structure based on the complexity of the task and the characteristics of the dataset.

In ResNeXt, all transformations have the same topology structure, thus having high scalability. However, limited by a fixed scale, the scope of perception is difficult to expand, resulting in limitations in the coverage of feature extraction for agricultural network security situation in digital economy. For providing a more detailed description of the agricultural network security situation, it is necessary to extract the elements of the agricultural network

security situation in digital economy from different perspectives. To address this issue, this paper optimize ResNeXt through model fusion. For overcoming the problem of poor feature extraction ability caused by the use of a single scale convolutional kernel in the areaof agricultural network security under the digital economy, MSCNN [22] is firstly proposed. This network significantly enhances the extraction efficiency of key elements related to agricultural network security in digital economy through the cross application of multi-scale convolution kernels. Therefore, the accuracy of agricultural network security situation awareness in digital economy is significantly improved. In addition, we introduce ECA [23] in each convolutional layer to perform weighted operations on the agricultural network security situation feature maps of each channel. Through this mechanism, valuable features for the current task can be strengthened while irrelevant features are weakened. In addition, this paper proposes a branch architecture with flexible adaptability, which supports setting the number of branches and convolution kernel size for each branch independently. This achieves accurate feature extraction of agricultural network security situation in digital economy by selecting appropriate branch numbers.

3.2.1 MSCNN

By using a multi-scale convolutional kernel cross structure, MSCNN can effectively extract the security situation features of agricultural network in digital economy from different perspectives, scales and directions. In addition, the Inception layer of each channel [24] is optimized using particle swarm optimization (PSO) [25] to enable MSCNN to adapt to different dimensions of agricultural network data in digital economy.

The architecture of MSCNN covers numerous branches, whose function is to capture the characteristics of agricultural network security situation under the digital economy from different scales. Each branch employs convolution kernels at diverse scales to fulfill the requirement of extracting features from agricultural network data across various scales. This leads to the presence of distinct neural network layers within each branch. ResNeXt generally uses fixed size convolution kernels to extract features of agricultural network data in digital economy from different perspectives. Nevertheless, this paper enhances this approach through the establishment of a multi branch and multi scale architecture. More precisely, we adaptively choose the size of convolution kernels in each branch according to the dimensional characteristics of the agricultural network security situation data. To achieve structural optimization and capture data features comprehensively, PSO is adopted to precisely ascertain the optimal number of layers for each individual branch. This method can ensure the efficient extraction of agricultural network security situation features from multiple scales in digital economy, effectively improving the overall performance of the network.

3.2.2 ECA

This paper uses ECA to optimize the performance of MSCNN-ResNeXt fusion module, for reducing computational complexity while maintaining performance. The traditional Squeeze-and-Excitation (SE) module [26] captures inter channel dependencies through two fully connected layers, although effective, but increases parameter and computational costs, especially in agricultural network in large-scale digital economy. In contrast, ECA utilizes 1D convolution to achieve local interaction between channels, avoiding dimensionality reduction operations, significantly reducing parameters, while retaining the ability to capture channel dependencies.

Similar to SE, ECA first conducts global average pooling on the input agricultural network security situation feature map $X \in \mathbb{R}^{C\times H\times W}$ to obtain the mean vector $X \in \mathbb{R}$ on the channel dimension, as shown in Equation 1.

$$y_c = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W} X_{c,i,j} \tag{1}$$

Unlike the fully connected layer of SE, ECA performs local interactions in the channel dimension through 1D convolution with a convolution kernel size of k, which can be dynamically regulated. This operation significantly reduces the computational cost, as shown in Equation 2.

$$z = Conv1D(y,k) \tag{2}$$

After a 1D convolution, the attention weight z is normalized using the Sigmoid function, as shown in Equation 3.

$$a_c = s(z_c) = \frac{1}{1+exp(-z_c)} \tag{3}$$

The final output of the agricultural network security situation feature map $\hat{X}$ in digital economy is obtained by applying attention weights to the original feature map, as shown in Equation 4.

$$\hat{X}_{c,i,j} = a_c \cdot X_{c,i,j} \tag{4}$$

3.3 Transformer

Transformer [27] surpasses traditional RNN and LSTM in handling long-range dependencies and parallel processing of input sequences. Transformer consists of two main parts, where the encoder is used to process the input sequence and the decoder is used to generate the output sequence [28]. To maintain the original order of input data, Transformer introduces positional encoding mechanism to ensure that the final input meets the condition of Input = input_embedding + positional_encoding. The position encoding mainly uses sin and cos alternately to represent the position, as shown in Equations 5, 6.

$$P_{(p,2i)} = sin\left(\frac{p}{1000^{2i/d_{model}}}\right) \tag{5}$$

$$P_{(p,2i+1)} = cos\left(\frac{p}{1000^{2i/d_{model}}}\right) \tag{6}$$

Where p represents the current position, 2i represents the even position, $2i+1$ represents the odd position, and d_{model} represents the dimension of the agricultural network security situation characteristics in the input digital economy.

The key idea of self attention mechanism is to determine the degree of association between each element and other elements by calculating the correlation between query, key and value [29]. Specifically, for each element in the input agricultural network sequence in digital economy, the self attention mechanism calculates

a set of attention weights by using it as a query and key and all elements as values. Attention weights represent the degree of attention that a query element pays to all other elements. They are assigned based on the correlation between the query element and other elements, with higher correlation resulting in greater weight. When calculating attention weights, the scaled dot product attention mechanism is usually used, where correlation is calculated through the dot product of queries and keys. The calculated attention weights are used to weight and sum the values to generate attention outputs. This means that each element can gather and aggregate information from other elements to obtain more global contextual information. In Transformer, self attention mechanism typically consists of multiple attention heads. Each attention head performs independent query key and value calculation, outputs its own attention weight and attention output. The outputs of multiple attention heads are cascaded together and finally projected and mapped through linear transformation.

The advantage of self attention mechanism lies in its ability to establish global correlations and adaptively allocate attention weights to different inputs, thereby better capturing the relationships in the sequence of agricultural network security situations in digital economy. This makes Transformer highly capable of modeling sequential tasks. The calculation method of the attention function is shown in Equation 7 below.

$$A_{attention}(Q,K,V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{7}$$

In this case, Q represents the query of attention, K represents the key of attention, V represents the value of attention, the function reduces the attention weight into the [0,1] range and $\sqrt{d_k}$ prevents the resulting dots from being too large.

The multi head attention mechanism can be understood as multiple independent attention mechanism working in parallel, each learning and focusing on different aspects of the input agricultural network security situation sequence in digital economy. Each attention mechanism has its own query, key, value and corresponding attention weights. Firstly, by linearly transforming the sequence of agricultural network security situation in the input digital economy, query, key and value are obtained. Then, each attention head calculates attention weights by computing the similarity between the query and the key, then weights and sums the values to obtain the attention representation of the head. Finally, the results of multiple attention heads are subjected to linear transformation and concatenation operations to obtain the final multi head attention representation. In this way, the model can focus on different parts of the input sequence from different perspectives, each head can learn different correlations. The multi head attention mechanism can capture different relationships in the sequence of agricultural network security situations in the input digital economy from multiple dimensions, improving the model's ability to capture important information in the sequence. The multi head attention mechanism is equivalent to the integration of h different self-attention and each convergence of attention is called the head. The h attention points are concatenated and transformed through learnable linear projections. Through this mechanism, the model can obtain unique features at different locations. The specific calculation of the multi head attention function can refer to Equation 8.

$$M_{MHA}(Q,K,V) = Concat(h_1,...,h_h)W^0 \tag{8}$$

Where Q, K, V represent the query, key and attention value of attention, W^0 represents the weight matrix, h represents the total number of heads and the Concat represents the splicing operation.

The feedback layer is a common structure in machine learning. It is used to introduce a feedback mechanism into the model, taking the model's output as input and further adjusting the learning and optimization process of the model [30]. Usually, the output of the model is compared with the real labels, the loss function is calculated and the parameters of the model are updated through backpropagation. However, the feedback layer feeds back the output of the model to the model itself, allowing the model to obtain additional information from previous prediction results. Specifically, the feedback layer can combine the output of the model as part of the input with the original input. In this way, the model can adjust the current learning process based on previous prediction results, thereby better utilizing previous information. In some tasks, using feedback layers can enhance the model's memory and contextual understanding abilities. By combining the output and input of the model, the model can gradually adjust its predictions to better adapt to the needs of agricultural network security situation awareness tasks in digital economy and improve overall performance. It should be noted that the design of the feedback layer needs to be determined based on specific tasks, appropriate adjustments need to be made during use to avoid issues such as overfitting or information overload. The feedback layer is a two-layer fully connected layer, with ReLu as the activation function for the first layer and no activation function for the second layer. The calculation formula is shown in Equation 9 below.

$$F(x) = max(0, XW_1 + b_1)W_2 + b_2 \tag{9}$$

Where X is the input, W_1, W_2 represent the weight matrix, b_1, b_2 represent the bias and the output matrix obtained by the feedback layer is consistent. The MSCNN-ResNeXt-Transformer uses the encoder part of the Transformer to optimize the MSCNN-ResNeXt fusion module. In addition to using the MSCNN-ResNeXt fusion module for feature extraction, techniques such as multi head self attention mechanism are also employed to extract and enhance data features, aiming to improve the accuracy of situational awareness. The MSCNN-ResNeXt-Transformer utilizes the self attention mechanism in Transformer to raise the operational precision of the MSCNN-ResNeXt fusion module. This mechanism endows the MSCNN-ResNeXt-Transformer with the ability to selectively focus on relevant agricultural network security situation features. The multi head self attention mechanism can analyze input sequences from multiple perspectives, enhancing the model's ability to learn complex agricultural network security situation patterns. Therefore, MSCNN-ResNeXt-Transformer performs well in agricultural network security situational awareness, achieving better performance compared to existing methods.

TABLE 1 Confusion matrix.

	Situation awareness is true	Situation awareness is false
Actually true	TP	FN
Actually false	FP	TN

4 Experiment and result analysis

4.1 Performance evaluation indicators for network security situational awareness

The system version of the experimental environment in this paper is Windows 10, the processor is Intel i7-7700k, the frequency is 4.2 GHz and the memory is 512 GB. The graphics card is a 24 GB RX 7900 XTX with a single core, using Python 3 as the main programming language, JQuery as the JavaScript tool library and based on the Pytorch framework. In addition, quantitative techniques are used to reduce computational and storage overhead. The weights of the model are quantized from 32-bit floating-point precision to 8-bit integers, reducing the model volume by 75% and computational complexity by nearly 50% while keeping the precision loss within 1%. This paper uses accuracy, recall, precision and F1-score as evaluation indicators for the assessment of network security situation awareness. As shown in Table 1, TP reflects the proportion of positive classes identified by the model that are actually positive classes. TN reflects how many of all true negative examples are correctly perceived as negative classes. FP reflects that the true labels of network samples are negative, but they are mistakenly judged as positive. FN reflects the number of network samples that are actually positive but incorrectly classified as negative.

According to the confusion matrix, we can obtain Equations for the following four evaluation indicators.

1. Accuracy measures the proportion of network data correctly identified by the model to all data in the entire test set, as shown in Equation 10.

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \tag{10}$$

2. Recall represents the ratio between the number of correctly classified data of a specific type and the total amount of data actually belonging to that category, as shown in Equation 11.

$$Recall = \frac{TP}{TP + FN} \tag{11}$$

3. Precision is the proportion of traffic data correctly classified into a specified type to the total number of network traffic data classified into this type, as shown in Equation 12.

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

4. F1 is a comprehensive indicator that combines information on accuracy and recall to evaluate the classification performance of the model. By balancing accuracy and recall, F1 provides a single measure to balance the relationship between the two, as shown in Equation 13.

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{13}$$

4.2 Experiments related to network security situation awareness

This paper is based on three datasets, they are MOORE, KDDCUP99 and WSN-DS. MOORE covers various core data of smart farms and typical agricultural network security threats, which can directly reflect the situational awareness ability of models in real agricultural environment. The network attack patterns in KDDCUP99 are highly compatible with the threats faced by agricultural network and can be used to evaluate the model's ability to identify common basic network attacks in agricultural network. The common network threats included in KDDCUP99, such as DoS attacks, unauthorized access and port scanning, are highly consistent with the basic security issues faced in agricultural networks, such as cloud platform intrusion and data transmission interference. But its limitation lies in the lack of farm specific threats, which cannot fully reflect the model's perception ability of agricultural scenario specific threats. WSN-DS includes threats such as false data injection, but its limitation is that it does not cover the compound threats unique to agriculture. WSN-DS is built on wireless sensor networks, which are widely used in modern agricultural precision monitoring. This can reflect the actual effectiveness of the model in ensuring the security of agricultural sensor network and provide validation for agricultural applicability.

Considering that the problem of imbalanced data distribution in binary classification is not obvious, this section focuses on conducting experiments on multi classification problems. Such experimental design not only helps to further explore and evaluate the performance of the model in handling complex situational awareness tasks, but also more clearly demonstrates the model's ability and effectiveness in handling data imbalance problems in various perception scenarios.

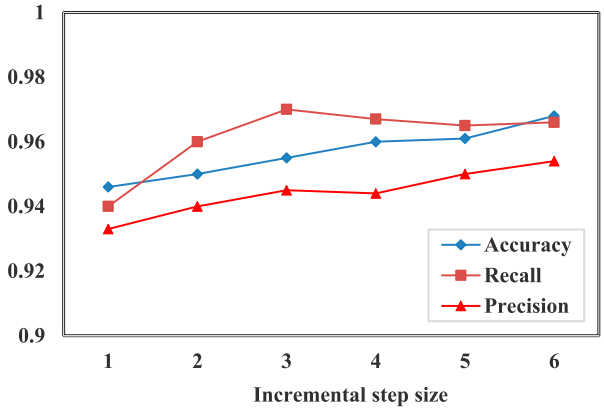

FIGURE 2
Performance of MSCNN-ResNeXt-Transformer at different incremental steps.

In Figure 2, the size of each incremental step is set to 1-6. In this experiment, each new category contained 4,000 samples. And the overall accuracy was above 0.94, indicating that MSCNN-ResNeXt-Transformer has high accuracy performance in agricultural network security situation awareness in the digital economy.

Through comparative experiments, this paper aims to comprehensively demonstrate the advantages of the proposed model in the field of network security, especially in security detection and situational awareness issues, and designs four sets of comparative experiments. The first comparative experiment is based on MOORE research. We select multiple baselines for network security situational awareness comparative experiments, including RNN [31], MSCNN [32], LSTM [33], ResNeXt [34], BiLSTM [35], Transformer [27] and MSCNN-ResNeXt-Transformer.

As shown in Table 2, MSCNN-ResNeXt-Transformer has significant advantages compared to other models. On MOORE, its accuracy, recall and precision are all higher than RNN, MSCNN, LSTM, ResNeXt, BiLSTM, Transformer and other models, reaching 0.928, 0.923 and 0.927, respectively. This indicates that MSCNN-ResNeXt-Transformer can accurately extract agricultural network data security features, accurately determine sample categories, has excellent coverage and accurate recognition capabilities for positive samples. Figure 3 is a visual representation of Table 2, where MSCNN-ResNeXt-Transformer is abbreviated as MSCNN.

Figure 3 shows that the accuracy of MSCNN-ResNeXt-Transformer reaches 0.928, which is about 3.23% higher than the second highest Transformer. Recall is 0.923, which is about 3.13% higher than Transformer. Precision is 0.928, which is about 5.94% higher than Transformer. Compared to the original ResNeXt, MSCNN-ResNeXt-Transformer uses MSCNN instead of a single scale convolution structure to comprehensively extract network security situation elements from multiple perspectives and scales, resulting in an improvement of about 12.76% in accuracy and about 9.62% in recall. This demonstrates its outstanding performance in agricultural network security situation awareness in digital economy. The second comparative experiment is based on the study of KDDCUP99.

TABLE 2 Comparison of situation awareness results based on MOORE.

Model	Accuracy	Recall	Precision
RNN	0.762	0.728	0.743
MSCNN	0.805	0.752	0.775
LSTM	0.849	0.815	0.832
ResNeXt	0.823	0.842	0.863
BiLSTM	0.81	0.853	0.866
Transformer	0.899	0.895	0.876
MSCNN-ResNeXt-Transformer	0.928	0.923	0.927

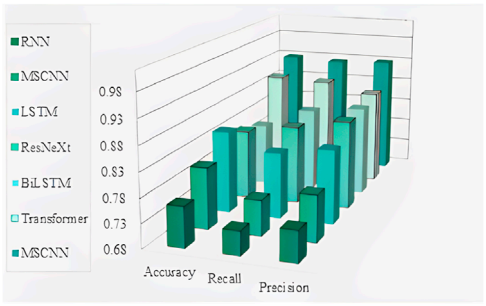

FIGURE 3
Comparison of network security situation awareness based on MOORE.

As shown in Table 3, on KDDCUP99, the accuracy of MSCNN-ResNeXt-Transformer is 0.939, recall is 0.955 and precision is 0.942, far exceeding other models. This indicates that MSCNN-ResNeXt-Transformer has good adaptability to different data distributions and features. It can stably operate in complex data environments and accurately perceive the security situation of agricultural network.

Figure 4 shows that MSCNN-ResNeXt-Transformer exhibits significant advantages on KDDCUP99. Compared with the single model, MSCNN-ResNeXt-Transformer replaces the single scale convolution structure with MSCNN, refines and characterizes the data processed by the improved ResNeXt using ECA and optimizes the network through the Transformer. The operation of this fusion model improves the accuracy of ResNeXt by about 12.72%, recall by about 15.76% and precision by about 11.35%. Compared with models such as RNN, MSCNN, LSTM and BiLSTM, MSCNN-ResNeXt-Transformer has outstanding leading advantages in various indicators, fully verifying its reliability in agricultural network security situation awareness in digital economy. The third comparative experiment is based on the study of WSN-DS.

As shown in Table 4, on WSN-DS, the accuracy of MSCNN-ResNeXt-Transformer is as high as 0.966, recall is 0.96 and precision is 0.952, demonstrating outstanding performance advantages. With its unique fusion architecture, MSCNN-ResNeXt-Transformer integrates the advantages of MSCNN, ResNeXt and Transformer,

TABLE 3 Comparison of situation awareness results based on KDDCUP99.

Model	Accuracy	Recall	Precision
RNN	0.775	0.772	0.758
MSCNN	0.812	0.805	0.805
LSTM	0.85	0.855	0.823
ResNeXt	0.833	0.825	0.846
BiLSTM	0.84	0.852	0.874
Transformer	0.894	0.908	0.883
MSCNN-ResNeXt-Transformer	0.939	0.955	0.942

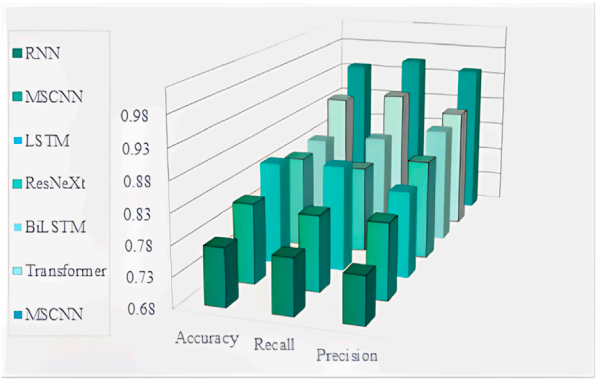

FIGURE 4
Comparison of network security situation awareness based on KDDCUP99.

TABLE 4 Comparison of situation awareness results based on WSN-DS.

Model	Accuracy	Recall	Precision
RNN	0.758	0.785	0.741
MSCNN	0.781	0.815	0.750
LSTM	0.813	0.827	0.799
ResNeXt	0.803	0.845	0.781
BiLSTM	0.843	0.85	0.826
Transformer	0.895	0.885	0.873
MSCNN-ResNeXt-Transformer	0.966	0.96	0.952

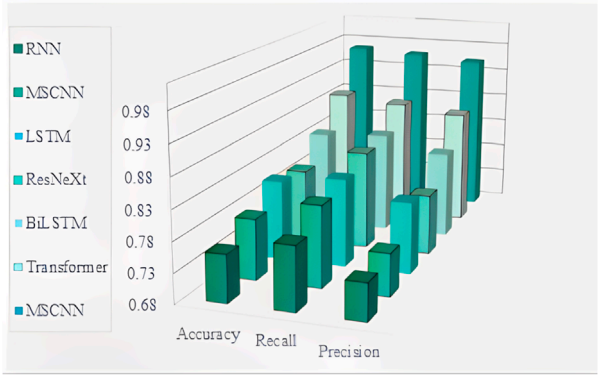

FIGURE 5
Comparison of network security situation awareness based on WSN-DS.

performs excellently in feature extraction, information fusion and complex pattern recognition. It can effectively respond to the complex data in the area of agricultural network security, providing a reliable method for agricultural network security situation awareness.

Figure 5 shows that the recall of MSCNN-ResNeXt-Transformer reaches 0.96, which is about 17.79% higher than MSCNN's 0.815 and about 16.08% higher than LSTM's 0.827. In terms of precision, MSCNN-ResNeXt-Transformer is 0.952, which is about 26.93% higher than MSCNN's 0.750 and about 19.15% higher than LSTM's 0.799. MSCNN-ResNeXt-Transformer significantly surpasses RNN, MSCNN, LSTM and other models, fully demonstrating its effectiveness in the field of agricultural network security situation awareness.

The fourth comparative experiment is based on the research of the comprehensive index F1, which compares the comprehensive performance of MSCNN-ResNeXt-Transformer with other models to evaluate the contribution of each component to the overall model situation awareness performance. It not only comprehensively verifies the effectiveness of MSCNN-ResNeXt-Transformer, but also clearly shows the progressiveness of introducing other methods, highlighting its advantages in feature extraction.

As shown in Table 5, compared with models such as RNN, MSCNN, LSTM and BiLSTM, MSCNN-ResNeXt-Transformer has outstanding leading advantages in various indicators, fully verifying its reliability in agricultural network security situational awareness in the digital economy.

Figure 6 shows that on MOORE, the F1 of MSCNN-ResNeXt-Transformer reaches 0.959, an increase of about 3.79% compared to Transformer's 0.924, an increase of about 6.67% compared to ResNeXt's 0.899 and a significant increase of about 23.11% compared to RNN's 0.779. On WSN-DS, the F1 of MSCNN-ResNeXt-Transformer is as high as 0.974, an increase of about 5.64% compared to Transformer's 0.922, an increase of about 9.20% compared to ResNeXt's 0.892 and an increase of about 26.17% compared to RNN's 0.772. MSCNN-ResNeXt-Transformer integrates ResNeXt and Transformer to comprehensively extract agricultural network security situation elements from multiple scales and perspectives. Then, the Transformer is used to optimize the network model, resulting in outstanding performance advantages on various datasets.

TABLE 5 Comparison of comprehensive experimental perception results.

Model	MOORE	KDDCUP99	WSN-DS
RNN	0.779	0.785	0.772
MSCNN	0.825	0.740	0.854
LSTM	0.848	0.870	0.887
ResNeXt	0.899	0.821	0.892
BiLSTM	0.883	0.885	0.934
Transformer	0.924	0.911	0.922
MSCNN-ResNeXt-Transformer	0.959	0.964	0.974

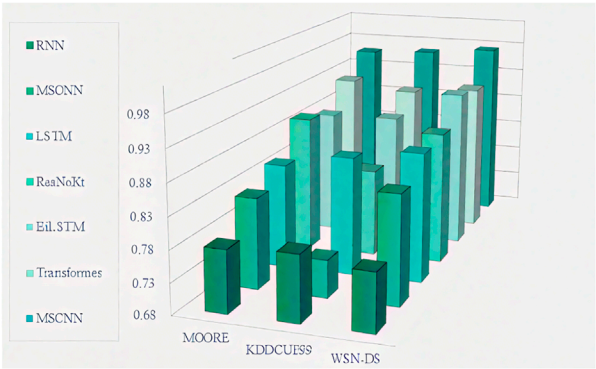

FIGURE 6
Comparison chart of comprehensive indicator perception results.

Through F1 analysis of the MOORE, KDDCUP99 and WSN-DS datasets, it is found that among the single components, Transformer performs the best, followed by ResNeXt and MSCNN is relatively weak. However, there is a significant gap between them and MSCNN-ResNeXt-Transformer, with an improvement of 3.5%–5.2% compared to the optimal single component. Specifically, the multi-scale convolutional structure of MSCNN provides rich initial features for the model, especially in complex data scenes, compensating for the shortcomings of other components in capturing local multi-scale features. ResNeXt's multi-branch grouped convolution enhances the non-linear expression ability of features and reduces feature redundancy. The self-attention mechanism of Transformer excels at modeling long-range temporal correlations and capturing feature dependencies across time steps in agricultural network security situations. The fusion of the three forms the MSCNN-ResNeXt-Transformer, fully verifying the necessity of each component and the rationality of the fusion strategy.

In terms of real-time response requirements for low-power devices, MSCNN-ResNeXt-Transformer uses 8-bit quantization to reduce parameter volume by 75% for low computing power and battery powered devices such as sensors and drone inspection modules. In terms of resisting seasonal data fluctuations, the multi-scale convolution kernel of MSCNN is used to capture seasonal features. And transformer is used to learn cross seasonal time series correlation, which is far better than a single model. In terms of false positives, ECA is used to focus on key features such as node data consistency to improve accuracy and provide practical technical support for agricultural network security.

5 Conclusion

This paper proposes a network security situation awareness method based on fusion model to address the problem of ineffective extraction of network security situation elements in agricultural network under the background of digital economy. MSCNN-ResNeXt-Transformer is a fusion model for network security situation awareness based on ResNeXt and Transformer. It uses the cross structure of MSCNN instead of single scale convolution, enabling ResNeXt to comprehensively extract agricultural network security situation elements in digital economy from multiple scales and perspectives. Meanwhile, MSCNN-ResNeXt-Transformer optimizes the network model using Transformer's encoder, improving the accuracy of agricultural network security situation awareness in digital economy. The experimental results show that MSCNN-ResNeXt-Transformer is significantly superior to traditional methods in attack detection accuracy and situational awareness effectiveness. This can effectively enhance the security protection capability of agricultural network.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

CZ: Conceptualization, Writing – original draft, Writing – review and editing, Project administration, Investigation, Visualization, Validation. ZL: Data curation, Writing – review and editing, Methodology, Software, Project administration, Resources.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

1. Hussain K, Rahmatyar AR, Riskhan B, Sheikh AM, Sindiramutty SR. Threats and vulnerabilities of wireless networks in the Internet of Things (IoT). In: 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC); 08-09 January 2024; Tandojam, Pakistan. IEEE (2024). p. 1–8.

2. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* (2023) 12(6):1333. doi:10.3390/electronics12061333

3. Bai Z, Miao H, Miao J, Xiao N, Sun X. Artificial intelligence-driven cybersecurity applications and challenges. *Innovative Appl AI* (2025) 2(2):26–33. doi:10.70695/aa1202502a09

4. Wang L, Parameshachari BD, Miao J. Digital economy oriented tourism industry data analysis in semantic IoT. *Internet Technology Lett* (2025) 8(4):e597. doi:10.1002/itl2.597

5. Sudha K, Nithyanandhan R, Girija P, Nalini M. Enhancing healthcare data security in the cloud: integrating ML-based intrusion detection systems. In: 2024 2nd World Conference on Communication and Computing (WCONF). IEEE (2024). p. 1–7.

6. Padmavathy R, Hurrah N. *Frontiers in cybersecurity: battling zero-day attacks and advanced persistent threats.* (2025).

7. Miao J, Ning X, Hong S, Wang L, Liu B. Secure and efficient authentication protocol for supply chain systems in artificial intelligence-based Internet of Things. *IEEE Internet Things J* (2025) 1. doi:10.1109/jiot.2025.3592401

8. Li M, Wang F, Jia X, Li W, Li T, Rui G. Multi-source data fusion for economic data analysis. *Neural Comput Appl* (2021) 33:4729–39. doi:10.1007/s00521-020-05531-0

9. Li X, Zhong Y. Exploration of a network security situation awareness model based on multisource data fusion. *Neural Comput Appl* (2023) 35(36):25083–95. doi:10.1007/s00521-023-08500-5

10. Li W, Zhang W, Liu B, Guo Y. The situation assessment of UAVs based on an improved whale optimization Bayesian network parameter-learning algorithm. *Drones* (2023) 7(11):655. doi:10.3390/drones7110655

11. Whelan J, Almehmadi A, El-Khatib K. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. *Comput Electr Eng* (2022) 99:107784. doi:10.1016/j.compeleceng.2022.107784

12. Da Silva LM, Ferrão IG, Dezan C, Espes D, Branco K. Anomaly-based intrusion detection system for in-flight and network security in uav swarm. In: 2023 International Conference on Unmanned Aircraft Systems (ICUAS); 06-09 June 2023; Warsaw, Poland. IEEE (2023). p. 812–9.

13. Benaddi H, Ibrahimi K, Benslimane A, Jouhari M, Qadir J. Robust enhancement of intrusion detection systems using deep reinforcement learning and stochastic game. *IEEE Trans Vehicular Technology* (2022) 71(10):11089–102. doi:10.1109/tvt.2022.3186834

14. Wang M, Song G, Yu Y, Zhang B. The current research status of AI-based network security situational awareness. *Electronics* (2023) 12(10):2309. doi:10.3390/electronics12102309

15. Wang C, Dong J, Guo G, Ren T, Wang X, Pan M. Security situational awareness of power information networks based on machine learning algorithms. *Connect Sci* (2023) 35(1):2284649. doi:10.1080/09540091.2023.2284649

16. Liu Z, Yang C, Liu Y, Ding Y. A BIPMU-based network security situation assessment method for wireless network. *Computer Stand and Inter* (2023) 83:103661. doi:10.1016/j.csi.2022.103661

17. He F, Zhang Y, Liu D, Dong Y, Liu C, Wu C, et al. Mixed wavelet-based neural network model for cyber security situation prediction using MODWT and Hurst exponent analysis. In: Network and System Security: 11th International Conference; August 21–23, 2017; Helsinki, Finland. Springer International Publishing (2017). p. 99–111.

18. Yin K, Yang Y, Yao C, Yang J. Long-term prediction of network security situation through the use of the transformer-based model. *Ieee Access* (2022) 10:56145–57. doi:10.1109/access.2022.3175516

19. Yang H, Zhang Z, Xie L, Zhang L. Network security situation assessment with network attack behavior classification. *Int J Intell Syst* (2022) 37(10):6909–27. doi:10.1002/int.22867

20. Ramadan RA, Emara AH, Al-Sarem M, Elhamahmy M. Internet of drones intrusion detection using deep learning. *Electronics* (2021) 10:2633. doi:10.3390/electronics10212633

21. Truong LNH, Clay E, Mora OE, Cheng W, Singh M, Jia X. Rotated Mask Region-based convolutional neural network detection for parking space management system. *Transportation Res Rec* (2023) 2677(1):1564–81. doi:10.1177/03611981221105066

22. Chen X, Fan J, Yu H, Xing Z, Yang G, Ding K. Research on fault diagnosis method based on the Markov transition field with enhanced properties and AM-MSCNN under different external environmental interference. *Struct Health Monit* (2025) 24(2):794–811. doi:10.1177/14759217241243353

23. Zhang Y, Zhan Q, Ma Z. EfficientNet-ECA: a lightweight network based on efficient channel attention for class-imbalanced welding defects classification. *Adv Eng Inform* (2024) 62:102737. doi:10.1016/j.aei.2024.102737

24. Alom MZ, Hasan M, Yakopcic C, Taha TM, Asari VK. Inception recurrent convolutional neural network for object recognition. *Machine Vis Appl* (2021) 32:28–14. doi:10.1007/s00138-020-01157-3

25. Jain M, Saihjpal V, Singh N, Singh SB. An overview of variants and advancements of PSO algorithm. *Appl Sci* (2022) 12(17):8392. doi:10.3390/app12178392

26. Chao X, Hu X, Feng J, Zhang Z, Wang M, He D. Construction of apple leaf diseases identification networks based on xception fused by SE module. *Appl Sci* (2021) 11(10):4614. doi:10.3390/app11104614

27. Han K, Wang Y, Chen H, Chen X, Guo J, Liu Z, et al. A survey on vision transformer. *IEEE Trans pattern Anal machine intelligence* (2022) 45(1):87–110. doi:10.1109/tpami.2022.3152247

28. Chen J, Mei J, Li X, Lu Y, Yu Q, Wei Q, et al. TransUNet: rethinking the U-Net architecture design for medical image segmentation through the lens of transformers. *Med Image Anal* (2024) 97:103280. doi:10.1016/j.media.2024.103280

29. Zheng X, Li X, Chen Z, Sun L, Yu Q, Guo L, et al. Enhanced self-attention mechanism for long and short term sequential recommendation models. *IEEE Trans Emerging Top Comput Intelligence* (2024) 8(3):2457–66. doi:10.1109/tetci.2024.3366771

30. Mienye ID, Swart TG. A comprehensive review of deep learning: architectures, recent advances, and applications. *Information* (2024) 15(12):755. doi:10.3390/info15120755

31. Hao S, Li HW, Ni YQ, Zhang W, Yuan L. State estimation in structural dynamics through RNN transfer learning. *Mech Syst Signal Process* (2025) 233:112767. doi:10.1016/j.ymssp.2025.112767

32. Liang J. Enhancing Fault diagnosis for chemical processes via MSCNN with hyperparameters optimization. *Syst Control Trans* (2025) 1712–7. doi:10.69997/sct.181373

33. Ławryńczuk M, Zarzycki K. LSTM and GRU type recurrent neural networks in model predictive control: a Review. *Neurocomputing* (2025) 632:129712. doi:10.1016/j.neucom.2025.129712

34. Zhou T, Zhao Y, Wu J. Resnext and res2net structures for speaker verification. In: 2021 IEEE Spoken Language Technology Workshop (SLT); 19-22 January 2021; Shenzhen, China. IEEE (2021). p. 301–7.

35. Riza BS, Yunita R, Rosnelly R. Comparative analysis of LSTM and BiLSTM in image detection processing. *J Wireless Mobile Networks, Ubiquitous Comput Dependable Appl (to be published)* (2024) 15:244–60. doi:10.58346/jowua.2024.i1.017