Journal of Network Intelligence ©2023 ISSN 2414-8105
Taiwan Ubiquitous Information Volume **8**, Number **4**, November **2023**

Intelligent Detection of Network Intrusion Based on Artificial Bee Colony Optimized Spiking Neural Network

Xueting Niu*

Dongchang College
Liaocheng University
Liaocheng 252000, P.R. China
xueting167@163.com

*Corresponding author: Xueting Niu

Received January 14, 2023, revised March 22, 2023, accepted May 8, 2023.

Abstract. *Intrusion Detection (ID) can monitor the operational state of a network to ensure the availability, integrity and confidentiality of system resources. Artificial intelligence and machine learning techniques applied to intrusion intelligence detection system can make the system more adaptable, self-learning and robust, which is an important direction of current intrusion detection research. As an advanced neural network structure, Spiking neural network(SNN) is often used for solving complex problems due to its good computational power, and has been applied in several fields. Therefore, this work proposes to apply Spiking neural network to intrusion detection system and model optimization using Artificial Bee Colony Algorithm (ABC) in order to improve the accuracy of intrusion detection. First, there are various neural network models based on the Spiking concept, and the Probabilistic Spiking neural network (PSNN) is chosen to build the intrusion detection model in this work. The proposed model is encoded by ignition time series and triggers an impulse response to achieve data delivery. Then, the artificial bee colony is constructed using the weights, dynamic thresholds, and forgetting parameters of the Spiking neural network, and the accuracy of intrusion detection is used as the fitness function of the ABC algorithm, so that the optimal individual can be obtained by continuously updating the fitness value of the individual colony. Finally, the network intrusion intelligence detection is completed with the PSNN model with optimal parameters. The experiments are divided into two parts: (1) performance verification of the proposed ABC-PSNN model; (2) network intrusion detection simulation. The experimental results show that the ABC-PSNN model has higher classification accuracy and stability compared with other Spiking neural network models and commonly used classification algorithms. Simulation results on the multiple datasest show that the ABC-PSNN-based intrusion detection model has a higher detection rate compared to other intrusion detection models.*

Keywords: network security; intrusion detection; Spiking neural network; artificial bee colony algorithm; probabilistic SNN

1. Introduction.

With the increase of incoming devices and data volume, the value of data available for deep mining in the network is highlighted. The integration of data from internal networks into external networks is increasing [1,2,3], but there is a greater risk of data transmission between internal and external networks [4,5]. Network security has become the primary factor affecting the upgrading of network services.

Network security technology research is developing rapidly, and intrusion detection, as an important strategic approach to network security defense, has a high application penetration rate [6,7,8]. Network intrusion detection systems can match the characteristics of common network attacks to determine the type of attack, thus providing data support for attack interception. However, new types of attacks are emerging, which provides a higher challenge to network intrusion detection technology. Network intrusion detection systems need to continuously learn and update attack types and achieve efficient and accurate detection [9,10]. Artificial intelligence and machine learning techniques, as tools for solving complex problems, have become the focus of research in network attack type detection in recent years. Spiking neural networks are often used for training solutions of complex problems due to their good computational power [11]. Spiking neural networks implement data transfer through pulse signals and encode them according to the pulse ignition time. The computational power of the Spiking neural network is significantly enhanced by the introduction of an exponential function for the output voltage solution. As an advanced neural network structure, Spiking neural network is often used for solving complex problems due to its good computational power, and has been applied in many fields. However, compared with the traditional neural network structure, the training of Spiking neural network is more complicated because it needs to determine the threshold and forgetting variables in addition to the connection weights of neurons.

Currently, the existing SNN models are solved not by using back propagation to determine the parameters, but by minimizing the difference for the actual ignition time, thus determining the stable Spiking neural network model. Therefore, this work proposes to apply Spiking neural networks to intrusion detection systems and to perform model optimization using Artificial Bee Colony Algorithm (ABC) in order to reduce the error of intrusion detection.

1.1. **Related Work.** Currently, there are two main categories of network security protection technologies: passive and active. Traditional firewalls benefit greatly from the proactive security protection provided by intrusion detection. High false alarm and missed alarm rates are a challenge for early intrusion detection systems. Researchers have suggested using machine learning approaches for intrusion prevention in the three primary ways of 1) induction, 2) categorization, and 2) data clustering as artificial intelligence advances. Zhao et al. [12] provide an exhaustive analysis of the advantages and disadvantages of various machine learning algorithms in intrusion detection systems.

While supervised learning-based intrusion detection models need a lot of labeled data, unsupervised learning-based intrusion detection models often have low classification accuracy. Therefore, semi-supervised models are widely used. Vahid et al. [13] proposed a hybrid network intrusion detection method based on K-mean clustering and multiple classifiers. Zong and Huang [14] used semi-supervised fuzzy C-mean clustering to implement network intrusion detection. The efficient fusion of a machine learning classification algorithm with a swarm intelligence optimization algorithm could improve the accuracy of intrusion detection which represents the new research topic. Gopalan and Krishnan [15] used an improved ant colony algorithm [16] to optimize the support vector machine thus improving the performance of network intrusion detection.

Currently, there are more studies on network intrusion detection using various neural network models. For example, Sohi et al. [17] used recurrent neural network algorithm for intrusion detection and improved RNN with the help of gated recurrent unit (GRU), which solved the problem that it takes a lot of time to solve the network parameters cyclically and effectively improved the efficiency of network intrusion detection. Raja et al. [18] used a lightweight GBM network for intrusion detection and achieved higher performance in detecting common attack types for large-scale traffic. Both of these studies use neural network models for common attack types detection, but their detection focus is slightly different. The former focuses more on the efficiency of detection, while the latter focuses more on the detection rate. Although both have high detection accuracy in common attack detection, there is still some room for improvement in their performance for more types of intrusion detection.

Currently, there are more researches on Spiking neural network model, Lee et al. [19] made a detailed analysis of the model structure and application scenarios based on Spike Timing Dependent Plasticity Spiking neural network (STDP-SNN). Amar et al. [20] used Long Short Term Memory (LSTM) structure to effectively improve the traditional impulsive neural network and proposed the LSTM-SNN model. It can be seen that there is still some room for improvement in the performance of the Spiking neural network model for solving complex problems.

1.2. Motivation and contribution.

In order to adapt to the needs of training and analysis of complex problems, it is often necessary to improve the traditional Spiking neural network effectively. This work takes the complex network intrusion detection problem as the entry point and optimizes the Spiking neural network model, using a combination of ABC and probabilistic Spiking neural network to achieve network intrusion detection. In this work, the main parameters of the probabilistic Spiking neural network are optimally solved by using ABC algorithm, which can not only obtain high performance in the detection of common attack types, but also still obtain high detection rate and stability in the non-useful attack types.

The main innovations and contributions of this work are shown below.

(1) As an advanced neural network structure, Spiking neural networks are often used for solving complex problems due to their good computational power. Therefore, this work proposes the application of advanced Spiking neural networks to intrusion detection systems.

(2) The ABC algorithm is used to optimally solve the main parameters of the probabilistic Spiking neural network, so this work can not only obtain high performance in the detection of common attack types, but also still obtain high detection rate and stability in the non-common attack types. According to the experimental findings, the ABC-PSNN model performs well in terms of classification precision. Simulation results on the multiple datasets show that the ABC-PSNN-based intrusion detection model has a higher detection rate compared with other intrusion detection models.

The rest of the paper is organized as follows: Section 2 introduces the basic principles of intrusion detection technology. Section 4 describes the proposed intelligent IDS based on ABC-PSNN model. Section 5 presents the performance verification of ABC-PSNN model. Section 6 presents the simulation example of network security. Section 7 concludes the paper.

2. The basic principles of intrusion detection technology.

2.1. Intrusion detection definition.

Intrusion has a great impact on the confidentiality, availability, and integrity of computers, as well as a huge.

The intrusion detection is a dynamic security technique. Intrusion detection is a dynamic security technology that monitors and analyzes system processes, checks the integrity of files on the system, identifies relevant attacks, identifies abnormal login patterns, and so on. An intrusion detection system is a combination of software and hardware that can perform intrusion detection.

Intrusion detection systems are capable of rapidly activating appropriate security protection mechanisms for access behaviors or abnormal operation patterns with attack characteristics [21,22]. The principle of anomaly intrusion detection system is shown in Figure 1.

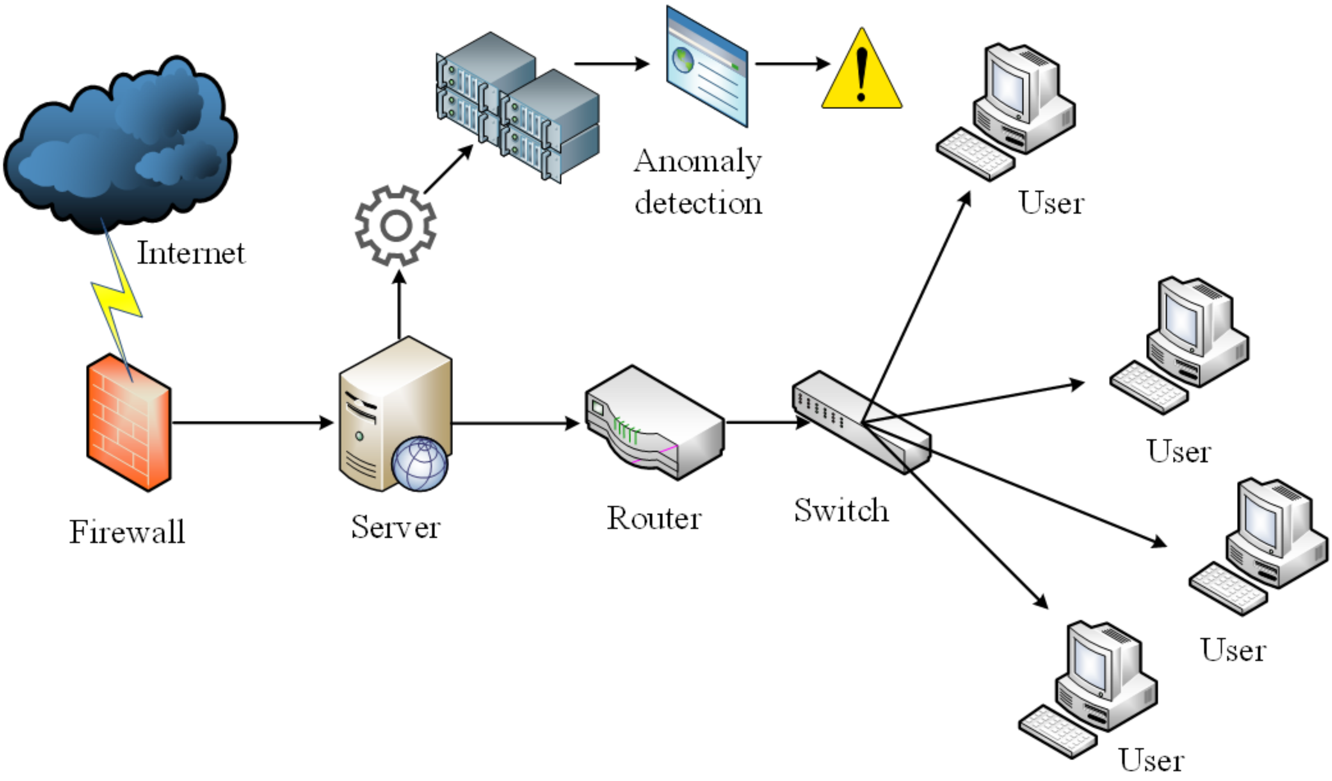

Figure 1. Principle of anomaly intrusion detection system

Based on the classification of data sources, intrusion detection systems can be classified as host-based IDS, network-based IDS, and application-based IDS. based on the classification of response methods, intrusion detection systems can be classified as active-responsive IDS and passive-responsive IDS. The active-responsive IDS system based on machine learning is studied in this work. Given the complexity of network systems, when experts are designing security systems, hand-coded rules usually fail to achieve the required high detection rate and low false alarm rate.

2.2. **Problems of IDSs.** Expert knowledge-based IDSs can only perform relevant matches for the attack types in their own pattern libraries. Therefore, when a new attack type appears, the expert knowledge-based IDS will fail. Expert knowledge-based IDSs are equivalent to supervised learning-based intrusion detection systems in machine learning. This type of attack system has high requirements for training datasets [23,24].

(1) Poor flexibility: When faced with a mixed type of network attack, the system will consider it as a normal type of attack, which will "contaminate" the training results during the training process and have a significant impact on the later detection results. Variations of this attack type will be considered as normal access behavior, and therefore, will greatly increase the false alarm rate.

(2) Poor generality: Since current intrusion detection systems and related statistical metrics need to be formed under specific environmental conditions, they have the characteristic of poor generality. At the same time, it is very difficult to invoke an already

built IDS in a constantly changing network environment. Since the current Internet is a dynamic network that keeps changing and new and mutated types of attacks keep appearing, there is an urgent need for a more intelligent and real-time intrusion detection system model.

3. Spiking neural network model.

3.1. Impulse response model.

Spiking neural networks contain three models, the most typical of which is the impulse response model, which is described mathematically below [25]. Assume that the voltage of the posterior synaptic neuron j is $u(t)$. When $u(t)$ is lower than the threshold τ , an output $t_j^{(f)}$ is triggered. The output sequence of the impulse response model is F_j.

$$F_j = \{t_j^{(f)}; 1 \leq f \leq n = t|u_j(t) = \tau\} \tag{1}$$

Assuming that all the anterior synaptic neurons i are contained in the set Γ_j, the ignition pulse affects the change in $u(t)$ as $P_j(t)$.

$$P_j(t) = \sum_{i \in \Gamma_j} \sum_{t_j^{(f)} \in F_i} w_{ij} \varepsilon_{ij}(t - \hat{t}_j, t - t_j^{(f)} - \Delta_{ij}^{ax}) + U_j^{ext} \tag{2}$$

Where w_{ij} is the weight, U_j^{ext} is the voltage change, ε_{ij} is the synaptic potential, $\underset{j}{\hat{t}}$ is the pulse output time, and Δ_{ij}^{ax} is the delay term.

Let $s = t - t_j^{(f)} - \Delta_{ij}^{ax}$ and use u_{rest} to represent the resting potential. The amount of change in the calculation process is $\eta_j(t - \underset{j}{\hat{t}})$. A common impulse response model $u_j(t)$ can be obtained by combining Equation (2).

$$u_j(t) = \eta_j(t - \underset{j}{\hat{t}}) + P_j(t) \tag{3}$$

On the basis of Equation (2), a simplified impulse response model (SRM_0) is commonly used as a substitute.

$$u_j(t) = \eta_j(t - \underset{j}{\hat{t}}) + \sum_{i \in \Gamma_j} \sum_{t_i^{(f)} \in F_i} w_{ij} \varepsilon_{ij}(t - t_j^{(f)}) + U_j^{ext} \tag{4}$$

A common representation of $\varepsilon_{ij}(t)$ is shown below.

$$\varepsilon_{ij}(t) = \frac{t - t_i^{(f)} - \Delta_{ij}^{ax}}{\tau} \cdot \exp(1 - \frac{t - t_i^{(f)} - \Delta_{ij}^{ax}}{\sigma}) \cdot H(t - t_i^{(f)} - \Delta_{ij}^{ax}) \tag{5}$$

Where σ is a constant and $H(\cdot)$ is a step function.

3.2. Probabilistic Spiking Neural Networks.

Among the common semi-supervised machine learning models, the voltage of probabilistic PSNNs based on $u(t)$ differs somewhat from the traditional definition.

$$u(t) = \sum_{i \in N} w_i \sum_{t'=0}^{t} \zeta(t - t') p_i^{t'} - \theta \sum_{k=0}^{t-1} \exp\left(-\frac{t-k}{\sigma}\right) p^k \tag{6}$$

Where, p_i^t is the probability of node i triggering a pulse at moment t, p^t is the probability of all nodes triggering a pulse at moment t, and ζ is a random number with the value range of (0,1), generally σ=1. denotes the weight between the current neuron and the i-th antecedent neuron.

$$w_i(t+1) = \eta x_i(t) \phi(y(t), \theta(t)) + (1 - \zeta) w_i(t) \tag{7}$$

Where η is a constant and x_i indicates the pulse duration.

$$\phi(y(t),\theta(t)) = y(t)(y(t)-\theta(t)) \tag{8}$$

Where y is the Spiking pulse ignition output sequence and θ represents the dynamic threshold.

$$\theta(t) = \frac{\sum\limits_{t'=t-h}^{t} y^2(t')\lambda^{t-t'}}{\sum\limits_{t'=t-h}^{t} \lambda^{t-t'}} \tag{9}$$

Where λ is the forgetting parameter.

When using Spiking neural network for training, it is very critical to set the four parameters reasonably, which directly affects the training effect of SNN. In the actual training process, it is very difficult to be able to find a suitable set of parameters (θ, w, η, λ) according to different samples. Therefore, this work tries to optimize the key parameters of SNN $(\theta, w, \eta, \lambda)$ by using population intelligence algorithm to obtain a better training performance of SNN.

4. Intelligent IDS based on ABC-PSNN model.

4.1. Artificial Bee Colony Algorithm.

The ABC algorithm performs an arithmetic solution by simulating a honey source search. We assume that the nectar source is i and the initial random position of the probe bee in the dth dimension is $\mathbf{X}_{id}$.

$$\mathbf{X}_{id} = \mathbf{L}_d + rand(0,1)(\mathbf{U}_d - \mathbf{L}_d) \tag{10}$$

Where $\mathbf{U}_d$ and $\mathbf{L}_d$ are the upper and lower bound ranges of the boundaries of the honey source search in the d-th dimension, respectively, and D denotes the total dimensionality,$d \in \{1,2,\cdots,D\}$.

The probe bee performs a nectar search at . The new nectar source is and is represented as shown below.

$$\mathbf{V}_{id} = \mathbf{X}_{id} + \varphi(\mathbf{X}_{id} - \mathbf{X}_{jd}) \tag{11}$$

Where $j \neq i$, ϕ values range from [-1,1] and $\mathbf{X}_{jd}$ is any position in the dth dimension in [$\mathbf{L}_d$,$\mathbf{U}_d$] (except for $\mathbf{X}_{id}$).
When the detecting bee detects a new nectar source $\mathbf{V}_i(\mathbf{V}_i = [\mathbf{V}_{i1}, \mathbf{V}_{i2}, \cdots, \mathbf{V}_{id}])$, it needs to calculate and update the adaptation f_i .

$$fit_i = \begin{cases} 1/(1+f_i), f_i \geq 0 \\ 1 + abs(f_i), otherwise \end{cases} \tag{12}$$

The fitness values of both old and new nectar sources were compared, and the result with the larger value was selected as the new source.

The detecting bee passes location information of multiple nectar sources to the following bee, and the following bee selects a preferred nectar source with probability p_i .

$$p_i = \frac{fit_i}{\sum\limits_{i=1}^{SP} fit_i} \tag{13}$$

Where SP is the number of all nectar sources.

We need to design a judgment strategy for the probe bee to search for nectar sources. When the number of iterations trial reaches the maximum number $I_{\max}$, then re-jump to

Equation (11), otherwise continue to find the optimal nectar source.

$$\mathbf{X}_i^{t+1} = \begin{cases} \mathbf{L}_d + rand(0,1)(\mathbf{U}_d - \mathbf{L}_d), trial \geq I_{\max} \\ \mathbf{X}_i^t, trial < I_{\max} \end{cases} \tag{14}$$

4.2. **Design of network intrusion detection system based on ABC-PSNN.** The model construction process of DBN is actually in the process of finding the optimal parameters.

And according to Section 3.2, it is known that in the process of finding the optimal parameters, it is necessary to go through several partial solutions. The quantity of solutions is directly related to the quantity of PSNN nodes. When the number of nodes is large, it takes a lot of training time to obtain the optimal solution by solving the partial derivatives one by one. Therefore, the ABC algorithm is considered in this work to solve the optimal parameters of PSNN $(\theta, w, \eta, \lambda)$. The ABC-PSNN based network intrusion detection system is shown in Figure 2.

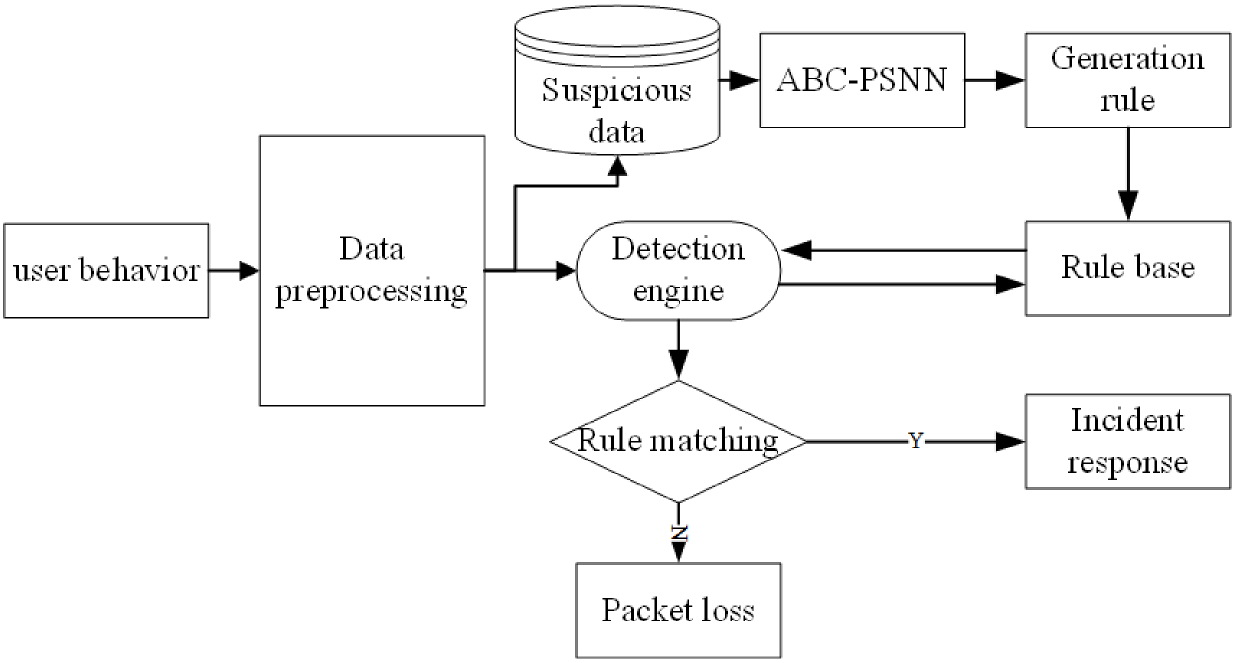

Figure 2. ABC-PSNN based Network Intrusion Detection System

4.3. **Process of Network Intrusion Detection.** First, all network intrusion detection samples are obtained and initial normalization is performed on them. Then, a PSNN-based network intrusion detection model is built and the network samples to be detected are input. Parameters such as PSNN weights and dynamic thresholds are extracted to construct the swarm.

Then, the position update optimization is performed by selecting the detection bee individual and the following bee individual of the swarm. The accuracy of intrusion detection is used as the fitness function to solve for the optimal individuals of the swarm, so as to obtain the optimal parameters suitable for PSNN classification. Finally, the network intrusion detection is performed using the PSNN optimized by ABC. The flow of network intrusion detection is shown in Figure 3.

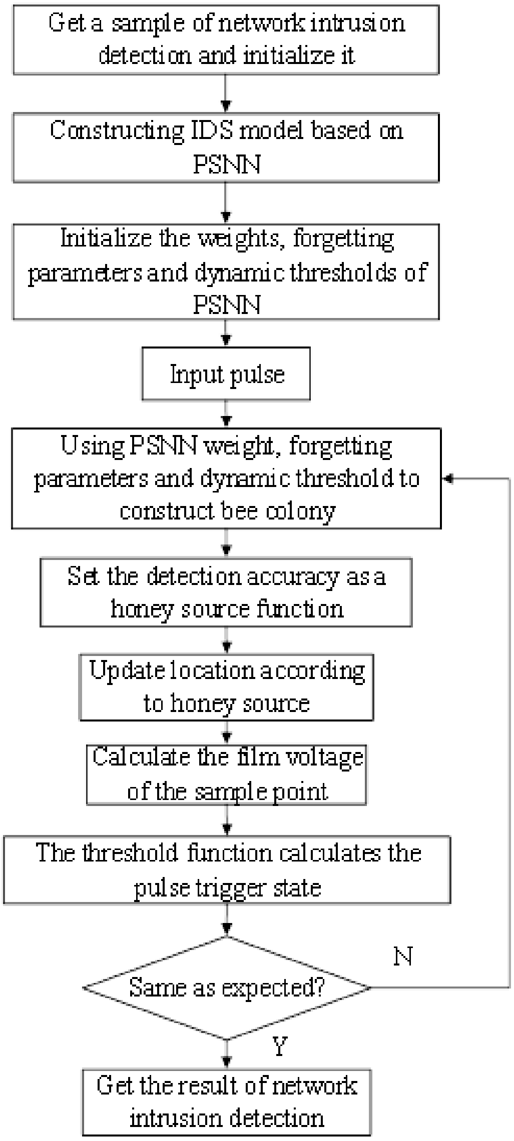
Get a sample of network intrusion detection and initialize it
Constructing IDS model based on PSNN
Initialize the weights, forgetting parameters and dynamic thresholds of PSNN
Input pulse
Using PSNN weight, forgetting parameters and dynamic threshold to construct bee colony
Set the detection accuracy as a honey source function
Update location according to honey source
Calculate the film voltage of the sample point
The threshold function calculates the pulse trigger state
Same as expected?
N
Y
Get the result of network intrusion detection

Figure 3. Intrusion detection flow based on ABC-PSNN

5. **Performance validation of the ABC-PSNN model.** To validate the performance of the ABC-PSNN model, simulation tests were conducted using four types of machine learning datasets from different domains. The classified sample data are shown in Table 1. First, the standard PSNN model is compared with the ABC-PSNN model in order to verify the effect of ABC parameter optimization on the classification performance

Table 1. Classification sample set

Sample set	Fields	Number of samples	Properties	Category
Langlog	Language Texts	1460	1004	75
Enron	Email Text	1702	1001	53
Scene	Images	2407	294	6
Emotion	Music files	1593	72	6

of PSNN. Second, the ABC-PSNN is compared with pairs of common impulsive neural network types. In the classification training of PSNN, the models used are all 4-layer structures.

5.1. **Optimization performance of ABC.** PSNN and ABC-PSNN are used for classification training, respectively. The classification accuracies of the two models are shown in Table 2. The mean classification accuracy of Langlog increased by 8.89%, while the mean classification accuracy of Enron increased by 6.67%. the mean classification accuracy of Scene increased by 8.34%, while the mean classification accuracy of Emotion increased by 6.69%. The mean classification accuracy of Scene improved by 8.34%, while the mean classification accuracy of Emotion improved by 6.69%. Among them, Langlog has the most significant improvement in accuracy, which indicates that different parameters of PSNN have a greater impact on the classification task of Langlog.

Table 2. Classification accuracy of PSNN and ABC-PSNN

Sample	**Models**	**Accuracy**		
		Minimum value	**Average value**	**Maximum value**
Langlog	PSNN	0.8475	0.8542	0.8611
	ABC-PSNN	0.9287	0.9301	0.9365
Enron	PSNN	0.8535	0.8637	0.8665
	ABC-PSNN	0.9189	0.9213	0.9231
Scene	PSNN	0.8560	0.8605	0.8692
	ABC-PSNN	0.9306	0.9323	0.9381
Emotion	PSNN	0.8572	0.8628	0.8667
	ABC-PSNN	0.9187	0.9205	0.9223

The classification RMSEs of the two models are shown in Table 3. It can be seen that for the 4-class classification sample set, the classification RMSE of PSNN decreases after the optimization of ABC algorithm. the mean RMSE of Langlog decreases by 2.52%, while the mean classification accuracy of Enron increases by 0.36%. the mean RMSE of Scene increases by 2.68%, while the mean RMSE of Emotion increases by The RMSE of Scene improved by 2.68%, while the RMSE of Emotion improved by 0.59%. Among them, the RMSE of Scene and Langlog decreased significantly, while the RMSE of the other two sample sets changed less. This indicates that there is no significant fluctuation in the classification RMSE of PSNN. Although the ABC algorithm can improve the classification stability of PSNN, the effect is not very significant, which may be because PSNN already has better adaptability to the 4-class sample set.

5.2. **Classification performance comparison of ABC-PSNN and other SNNs.** The performance simulations were performed using ABC-PSNN, STDP-SNN and LSTM-SNN for four classes of classification sample sets, respectively, and the results are shown in Table 4, Table 5, Table 6 and Table 7.

It can be seen that after ABC optimization, the ABC-PSNN algorithm significantly outperforms the other 2 impulsive neural network algorithms in the main 4 classification metrics. In terms of classification accuracy, the ABC-PSNN model obtained the highest

Table 3. Classification RMSE of PSNN and ABC-PSNN

Sample	**Models**	**RMSE**		
		Minimum value	**Average value**	**Maximum value**
Langlog	PSNN	0.8311	0.8342	0.8381
	ABC-PSNN	0.8111	0.8132	0.8144
Enron	PSNN	1.0283	1.0305	1.0332
	ABC-PSNN	1.0252	1.0268	1.0283
Scene	PSNN	1.1215	1.1366	1.1293
	ABC-PSNN	1.1052	1.1061	1.1071
Emotion	PSNN	1.1604	1.1621	1.1653
	ABC-PSNN	1.1531	1.1552	1.1568

Table 4. Classification accuracy of PSNN and ABC-PSNN

Dataset	**Models**		
	STDP-SNN	**LSTM-SNN**	**ABC-PSNN**
Langlog	0.8226	0.8415	0.9301
Enron	0.8317	0.8562	0.9213
Scene	0.8144	0.8479	0.9323
Emotion	0.8103	0.8632	0.9205

Table 5. Classification recall rate

Dataset	**Models**		
	STDP-SNN	**LSTM-SNN**	**ABC-PSNN**
Langlog	0.8151	0.8327	0.9215
Enron	0.8237	0.8347	0.9049
Scene	0.8025	0.8219	0.8927
Emotion	0.7962	0.8525	0.8883

Table 6. Classification F1 values

Dataset	**Models**		
	STDP-SNN	**LSTM-SNN**	**ABC-PSNN**
Langlog	0.8023	0.8110	0.9125
Enron	0.8016	0.8212	0.9105
Scene	0.7925	0.8124	0.8901
Emotion	0.7703	0.8138	0.8824

accuracy of 0.9323 on Scene, while STDP-SNN obtained an accuracy of only 0.8103 on Emotion. this shows that the traditional impulse neural network algorithm still has large shortcomings when used for classification. In the specific application environment, a suitable impulse neural network model needs to be selected according to the needs.

Table 7. Classification RMSE

Dataset		Models	
	STDP-SNN	LSTM-SNN	ABC-PSNN
Langlog	0.8491	0.8380	0.8132
Enron	1.0916	1.1083	1.0268
Scene	1.3892	1.3765	1.1061
Emotion	1.4324	1.4221	1.1552

Moreover, the traditional model has to be properly optimized according to the model training performance needs.

6. Simulation examples of network security.

6.1. Simulation environment.

First, the detection performance of ABC-PSNN model for different attack types is verified. Secondly, common deep learning algorithms are compared with ABC-PSNN. parameters of four network intrusion detection sample sets are shown in TABLE 8. The experimental hardware configuration is: AMD R5-5600G 3.9GHz CPU, 8 GB RAM, 1 T hard disk. The software configuration is: Windows 10 OS, MATLAB 2012, CloudSim 4.0. All sample sets were divided into training data with markers and test data without markers. The attack types are DOS, R2L, U2R, and PROBE. There is a large disparity in the number of different attack types in the four types of sample sets, and the common attack types in all four data sets account for more than 80%, so the four common attack types are mainly selected for performance simulation.

Table 8. Network intrusion detection samples

Data set name	Number of samples	Number of attacks
KDD cup99	45063	13
Masquerading User Data	40126	12
HTTP DATASET CSIC (2010)	37634	10
ADFA IDS Datasets	39721	11

6.2. Data pre-processing.

The data should be normalized at the data pre-processing step in order to prevent the outcomes of intrusion detection from being impacted by the reality that the intrusion data may not match the kind of intrusion have varying numbers of characteristics and units of measure, respectively.

$$new\_s[j] = \frac{\log\left(\frac{ide}{\min\_col+dis}\right) + \log\left(col + dis\right)}{\log\left(\frac{ide}{\min\_col+dis}\right) + \log\left(\max\_col + dis\right)} \tag{15}$$

Where ide denotes the mean value of the standard deviation of the variable column, dis denotes the missing value of the standard deviation of the variable column, min_col and max_col denote the minimum and maximum values of the variable column, respectively.

Table 9. Intrusion detection performance (single type)

Dataset	**Type**	**Detection rate %**	**False alarm rate %**
KDD cup99	Normal	98.87	2.23
	PROBE	99.15	1.92
	R2L	99.31	1.73
	DOS	99.62	1.85
	U2R	99.05	1.67
Masquerading User Data	Normal	98.55	2.14
	PROBE	99.12	1.86
	R2L	99.25	1.69
	DOS	99.44	1.78
	U2R	99.16	1.58
HTTP DATASET CSIC (2010)	Normal	98.93	2.05
	PROBE	99.24	1.86
	R2L	99.62	1.63
	DOS	99.62	1.76
	U2R	99.83	1.53
ADFA IDS Datasets	Normal	99.06	2.23
	PROBE	99.37	1.73
	R2L	99.49	1.61
	DOS	99.58	1.58
	U2R	99.73	1.32

6.3. **Detection performance for different types of attacks.** Intrusion detection simulations are performed for samples of different attack types. The detection performance of the ABC-PSNN model for a single type of network intrusion attack is shown in Table 9. It can be seen that the ABC-PSNN model has a detection rate higher than 98.5% for all four common attack types in all sample sets, and the false alarm rate also stays within 3%, which indicates that the ABC-PSNN model has high applicability for common attack type detection and is more suitable for intrusion detection of a single type of attack.

6.4. **Detection Performance of Mixed Type Attacks.** The small number of R2L and U2R samples of HTTP DATASET CSIC and ADFA IDS Datasets leads to uneven number of samples for hybrid attack detection. Therefore, only 2 sets, KDD cup99 and Masquerading User Data, are selected for mixed attack detection in this work, and the results are shown in Table 10. The detection rate of ABC-PSNN model for mixed attack types remains above 98To verify the optimization effect of ABC algorithm on network intrusion detection performance, PSNN and ABC-PSNN are used to simulate intrusion detection on the 4-class sample set, respectively. Compared with the PSNN model, the detection rate of ABC-PSNN model on the 4-class sample set is improved by 7.72%, 7.92%, 7.13% and 6.02%, respectively, while the false alarm rate is reduced by 33.01%, 29.93%, 28.57% and 29.69%, respectively. According to the simulation findings, intrusion detection performance is significantly improved after the optimization of ABC. the RMSE values of the ABC-PSNN model are significantly lower than those of the PSNN model. The stability of network intrusion detection is enhanced significantly after ABC optimization, which is mainly because the ABC algorithm obtains better PSNN model parameters $(\theta, w_i, \eta, \lambda)$.

Table 10. Intrusion detection performance (mixed type)

Dataset	Type	Detection rate %	False alarm rate %
KDD cup99	Normal+PROBE	98.63	2.49
	Normal+ DOS	98.06	2.83
	Normal+ R2L	98.24	2.55
	Normal+ U2R	98.15	2.16
	PROBE+ DOS	99.13	1.68
	PROBE+ U2R	99.27	1.53
	PROBE+ R2L	99.14	1.78
	DOS+ U2R	98.91	2.04
	DOS+ R2L	98.93	1.56
	U2R+R2L	98.62	1.71
Masquerading User Data	Normal+PROBE	98.34	2.53
	Normal+ DOS	99.18	1.67
	Normal+ R2L	98.91	1.93
	Normal+ U2R	98.58	2.11
	PROBE+ DOS	99.12	1.49
	PROBE+ U2R	99.33	1.32
	PROBE+ R2L	98.62	2.41
	DOS+ U2R	99.06	2.08
	DOS+ R2L	98.96	1.89
	U2R+R2L	98.09	2.37

6.5. **Comparison of four network intrusion detection models.** To further validate the detection performance of the ABC-PSNN model, it was simulated and compared with the commonly used deep learning networks CNN [26], LSTM [27], and GAN [28], as shown in Figure 4 to Figure 7. The evaluation metrics are detection rate and RMSE.

It can be seen that the detection rates of all four deep learning models are higher than 0.9. When reaching stability, the CNN model has the lowest detection rate, the other three models are very close to each other, and the ABC-PSNN model is slightly higher. In terms of detection time, the differences among the four models are small. In terms of detection rate of Masquerading User Data set, ABC-PSNN ¿ GAN ¿ LSTM ¿ CNN. the detection rate of ABC-PSNN has a significant advantage over the other 3 models, and its detection rate is close to 1. the detection rates of GAN and LSTM are very close, while CNN is worse. In terms of false alarm rate, the ABC-PSNN model slightly outperforms the other three deep learning models, but the difference basically stays within 1%. Finally, in terms of RMSE performance, ABC-PSNN has a clear advantage with its value staying within 0.015, while the RMSE values of the other 3 models are all above 0.03.

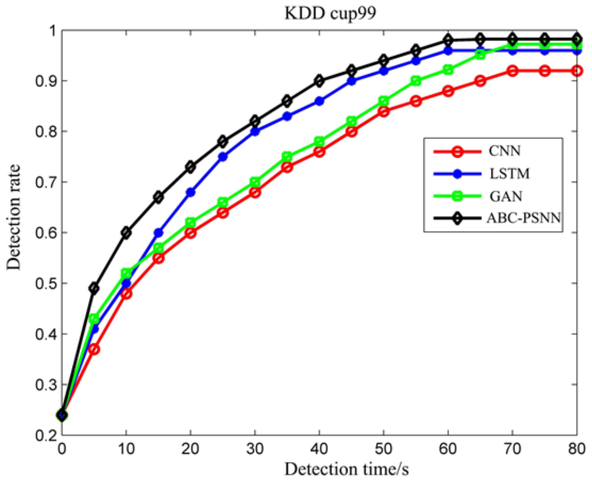

Figure 4. KDD cup99

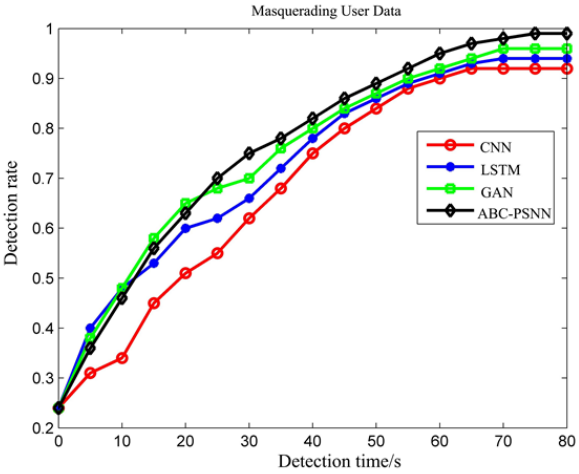

Figure 5. Masquerading User Data

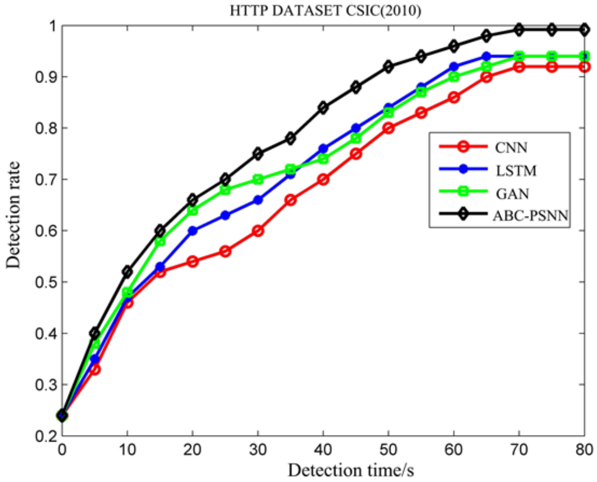

Figure 6. HTTP DATASET CSIC(2010)

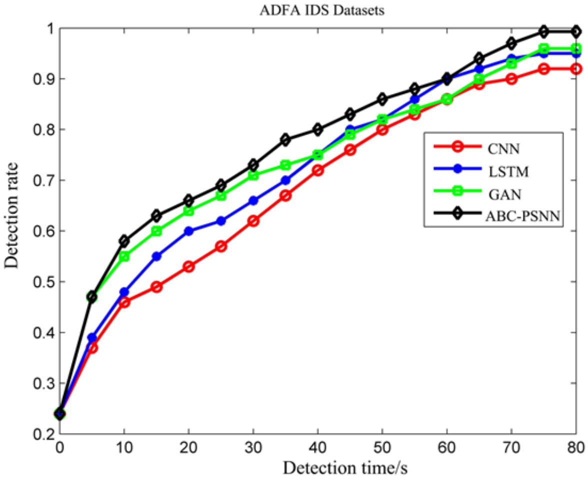

Figure 7. ADFA IDS Datasets

7. Conclusion.

In this work, the ABC-PSNN model is used for semi-supervised network intrusion detection, and the difficult classification problem is effectively solved by the impulse-triggered response of the PSNN model, while the ABC algorithm can effectively optimize the key parameters of the PSNN, thus improving the classification performance of the PSNN model. By comparing with the commonly used deep learning models, the ABC-PSNN model has obvious advantages in the classification and recognition of network intrusion detection, showing higher classification accuracy and stability. However, for mixed attack types, the ABC-PSNN model still does not perform well enough and there are certain false detection cases. Subsequent research will further differentiate the main parameters of the ABC to increase the classification efficiency of the ABC-PSNN model, so as to enhance the adaptability of large-scale network security protection.

Acknowledgement. This work is supported by project of Cooperative education project of the ministry of education (201901173025) and shandong provincial department of education (M2022285).

REFERENCES

[1] T.-Y. Wu, Q. Meng, L. Yang, “Saru Kumari, Matin Pirouz Nia, Amassing the Security: An Enhanced Authentication and Key Agreement Protocol for Remote Surgery in Healthcare Environment,” *Computer Modeling in Engineering and Sciences*, vol. 134, no. 1, pp. 317-341, 2023.

[2] H. Li, K. Ota, and M. X. Dong, “Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing,” *IEEE Network*, vol. 32, no. 1, pp. 96-101, 2018.

[3] T.-Y. Wu, F. F. Kong, L. Y. Wang, Y.-C. Chen, S. Kumari, and J.-S. Pan, “Toward Smart Home Authentication Using PUF and Edge-Computing Paradigm,” *Sensors*, vol. 22, no. 23, 9174, 2022.

[4] J. Q. Gao, H. Y. Zou, F. Q. Zhang, and T. Y. Wu, “An intelligent stage light-based actor identification and positioning system,” *International Journal of Information and Computer Security*, vol. 18, no. 1/2, pp. 204–218, 2022.

[5] J. Sun, “Computer Network Security Technology and Prevention Strategy Analysis,” *Procedia Computer Science*, vol. 208, pp. 570-576, 2022.

[6] C.-M. Chen, S. Lv, J. Ning, and J. M.-T. Wu, “A Genetic Algorithm for the Waitable Time-Varying Multi-Depot Green Vehicle Routing Problem,” *Symmetry*, vol. 15, no. 1, 124, 2023.

[7] N. Priyadarshi, S. Padmanaban, J. B. Holm-Nielsen, M. S. Bhaskar, and F. Azam, “Internet of things augmented a novel PSO -employed modified zeta converter-based photovoltaic maximum power tracking system: hardware realization,” *IET Power Electronics*, vol. 13, no. 13, pp. 2775-2781, 2020.

[8] A. L. H. P. Shaik, M. K. Manoharan, A. K. Pani, R. R. Avala, and C.-M. Chen, “Gaussian Mutation–Spider Monkey Optimization (GM-SMO) Model for Remote Sensing Scene Classification,” *Remote Sensing*, vol. 14, no. 24, 6279, 2022.

[9] R. Kumar and R. Tripathi, ”DBTP2SF: A deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems,” *Transactions on Emerging Telecommunications Technologies*, vol. 5, no. 8, pp. 109-121, 2021.

[10] Z. Ni, Q. Li, and G. Liu, “Game-Model-Based Network Security Risk Control,” *Computer*, vol. 51, no. 4, pp. 28-38, 2018.

[11] A. A. Abusnaina, R. Abdullah, and A. Kattan, ”Supervised Training of Spiking Neural Network by Adapting the E-MWO Algorithm for Pattern Classification,” *Neural Processing Letters*, vol. 49, pp. 661-682, 2018.

[12] M. W. Zhao, G. W. Wei, C. Wei, and Y. F. Guo, ”CPT-TODIM method for bipolar fuzzy multi-attribute group decision making and its application to network security service provider selection,” *International Journal of Intelligent Systems*, vol. 36, no. 5, pp. 1943-1969, 2021.

[13] S. Vahid and M. Ahmadzadeh, “KCMC: A Hybrid Learning Approach for Network Intrusion Detection using K-means Clustering and Multiple Classifiers,” *International Journal of Computer Applications*, vol. 124, no. 9, pp. 18-23, 2015.

[14] Y. S. Zong and G. Y. Huang, “Application of artificial fish swarm optimization semi-supervised kernel fuzzy clustering algorithm in network intrusion,” *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 2, pp. 1619–1626, 2020.

[15] S. H. Gopalan and R. R. Krishnan, ”Trust Based Fuzzy Aided ACO for Optimal Routing with Security in MANET,” *Asian Journal of Research in Social Sciences and Humanities*, vol. 6, 529, 2016.

[16] K. S. Sreejini and V. K. Govindan, “Severity Grading of DME from Retina Images: a Combination of PSO and FCM with Bayes Classifier,” *International Journal of Computer Applications*, vol. 81, no. 16, pp. 11-17, 2013.

[17] S. M. Sohi, J.-P. Seifert, and F. Ganji, “RNNIDS: Enhancing Network Intrusion Detection Systems through Deep Learning,” *Computers & Security*, vol. 6, no. 22, 102151, 2020.

[18] G. Raja, S. Anbalagan, G. Vijayaraghavan, and S. Theerthagiri, ”SP-CIDS: Secure and Private Collaborative IDS for VANETs,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4385-4393, 2021.

[19] C. Lee, W. Y. Lee, S. Han, and C. Park, ”ECG-Based Arrhythmia Detection SNN Algorithm Using STDP and Spike Inference for Smart Health City,” *The Journal of Korean Institute of Communications and Information Sciences*, vol. 45, no. 12, pp. 2193-2201, 2020.

[20] A. Shrestha, K. Ahmed, Y. Wang, D. P. Widemann, and A. T. Moody, ”Modular Spiking Neural Circuits for Mapping Long Short-Term Memory on a Neurosynaptic Processor,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 8, no. 4, pp. 782-795, 2018.

[21] P. V. Pramila and M. Gayathri, ”Analysis of Accuracy in Anomaly Detection of Intrusion Detection System Using Naïve Bayes Algorithm Compared Over Gaussian Model,” *ECS Transactions*, vol. 107, no. 1, pp. 13977-13991, 2022.

[22] Y. Yuan, J. Shao, M. Zhong, and H. Wang, “Paper Information Recording and Security Protection Using Invisible Ink and Artificial Intelligence,” *ACS Applied Materials & Interfaces*, vol. 13, no. 16, pp. 19443–19449, 2021.

[23] R. Casado-Vara and J. Corchado, ”Distributed e-health wide-world accounting ledger via blockchain,” *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 3, pp. 2381-2386, 2019.

[24] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, ”Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network,” *Sensors*, vol. 20, no. 10, pp. 2798-2801, 2020.

[25] Q. Fu and H. Dong, ”Breast Cancer Recognition Using Saliency-Based Spiking Neural Network,” *Wireless Communications and Mobile Computing*, vol. 4, pp. 1-17, 2022.

[26] G. Mao, Z. Z. Zhang, B. Qiao, and Y. B. Li, ”Fusion Domain-Adaptation CNN Driven by Images and Vibration Signals for Fault Diagnosis of Gearbox Cross-Working Conditions,” *Entropy*, vol. 24, no. 1, 119, 2022.

[27] E. Mushtaq, A. Zameer, M. Umer, and A. A. Abbasi, ”A two-stage intrusion detection system with auto-encoder and LSTMs,” *Applied Soft Computing*, vol. 121, 108768, 2022.

[28] K. Liu, Z. Ye, H. Guo, and D. Cao, ”FISS GAN: A Generative Adversarial Network for Foggy Image Semantic Segmentation,” *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 8, pp. 1428-1439, 2021.