Stochastic Nonlinear Analysis of Internet of Things Network Performance and Security

Junzhou Li[1], Feixian Sun[2]*
Information Management Center, Kaifeng University, Kaifeng, China[1]
School of Electronics and Internet of Things, Henan Polytechnic, Zhengzhou, China[2]
Zhengzhou Key Laboratory of Electronic Intelligent Sensor Application Technology, Zhengzhou, China[2]

***Abstract*—Aiming at the problem of poor effect of traditional Internet of Things network performance and security analysis methods, the research uses support vector machine for Internet of Things network security situation assessment. It also introduces the grey wolf optimization algorithm improved by genetic algorithm to optimize it, and designs a stochastic nonlinear integration of Internet of Things network performance algorithm. The results revealed that the mean absolute error, root mean square error, and mean absolute percentage error of the integrated algorithm were 0.0064, 0.041, and 0.0013, respectively, in the performance test. It was significantly lower than that of the other four algorithms, which proved that its prediction accuracy was higher. The recall of the integrated algorithm was 93.7%, and the F1 value was 0.94, which was significantly higher than the other comparative algorithms, proving its better comprehensive performance. In the analysis of practical application effect, when access control was performed by the integrated algorithm, the predicted curve basically overlapped with the actual curve, which proved its better fitting performance. The communication overhead of the integrated algorithm was 81.3 KB, which was significantly lower than the other two calculations. The average communication time of the integrated algorithm was 3.59 s, which was lower than the other two algorithms, proving that it can effectively reduce the communication cost and delay. The integrated algorithm can effectively improve the performance of Internet of Things network security situation assessment, which provides reliable technical support for the security protection of Internet of Things network and has important practical application value.**

Keywords*—Internet of Things; security; stochastic nonlinearity; support vector machines; grey wolf optimization algorithm

I. Introduction

The Internet of Things (IoT) has emerged as a link between the digital and physical worlds as a result of the rapid advancement of information technology [1]. From smart homes and smart cities to the industrial Internet, IoT is changing the way people live and work. It enables real-time data collection, transmission, and processing by connecting disparate devices and systems, creating unprecedented opportunities to improve efficiency, reduce costs, and optimize resource allocation. However, since IoT involves the communication of a large number of devices distributed all over the world and operating in complex and variable environments, the randomness and uncertainty of IoT network traffic increases significantly [2, 3]. Meanwhile, as the security protection mechanism of IoT is still imperfect, the network attack surface has expanded, making the network security threat increasingly serious [4]. The widespread adoption of IoT poses a serious challenge to network performance and security. Therefore, the inherent stochastic and nonlinear characteristics must be fully considered when studying the performance and security of IoT networks. In current research, network performance analysis of IoT mostly adopts static models or dynamic monitoring methods based on specific assumptions, while security analysis relies on traditional means such as vulnerability scanning and code review [5]. However, these methods are challenging to implement effectively due to the nonlinear and separable characteristics of IoT traffic, which can result in suboptimal classification accuracy. The incorporation of random disturbances, such as equipment failures and sudden traffic surges, into the model remains incomplete, resulting in substantial deviations in prediction outcomes. Meanwhile, these methods require a significant amount of computing resources, which conflicts with the low-power requirements of IoT edge devices. Therefore, the present focus of relevant researchers is on the development of an analysis method that takes into account the inherent randomness and nonlinear characteristics of the IoT environment. This method is intended to address the complexity and uncertainty that arise from massive device communication in security situation assessment. In this context, a security situation assessment method for the IoT network was developed based on an improved support vector machine (SVM) to address the above issues. To optimize the SVM parameters, a parameter optimization method combining genetic algorithm and improved grey wolf optimization algorithm (GA-IGWO) was proposed to improve the classification accuracy and computational efficiency. Compared with traditional methods, this algorithm can significantly improve the accuracy and efficiency of network performance evaluation by fully considering the randomness and nonlinear characteristics in the IoT environment, while reducing communication costs and delays. It has important theoretical value and practical application significance for improving the security and performance of IoT networks. The innovation of the research lies in the design of an integrated algorithm that effectively improves the performance of IoT networks and provides reliable technical support for the security protection of IoT networks.

This study mainly includes six sections. The first section is the background of IoT network performance and security. The second section is the research progress in the field of IoT network security situation assessment in recent years. The third section is dedicated to the design of an IoT network security situation assessment algorithm based on ISVM-GA-IGWO. This section introduces the IoT network security situation

This study was supported by the Science and Technology Planning Project of Henan Province, China (Grant No. 242102320167).

assessment method based on ISVM and the ISVM parameter optimization method based on GA-IGWO. The fourth section is the effectiveness analysis of the IoT network security situation assessment algorithm based on ISVM-GA-IGWO. Through performance analysis and practical application effect analysis, the superiority of the proposed algorithm is verified. The fifth section is a discussion that delves into the advantages of the proposed method. The sixth section is the conclusion, which summarizes the main results of the research, points out the limitations of the current methods, and suggests future research directions.

II. Related Works

As technology continues to develop, the IoT has become a vital component of people's daily lives, facilitating the control and management of a wide range of devices through Internet connectivity. However, through IoT devices, people's personal information can be collected, stored and transmitted, and personal privacy is at great risk. Therefore, protecting the security of IoT networks has become a hot research topic for related workers. Numerous academics have studied IoT network security condition assessment in recent years. An interpretable deep learning (DL)-based intrusion detection system was created by Oseni et al. to identify network threats in IoT networks. To safeguard IoT networks and create more resilient systems, specialists relied on the decisions made by the DL-based intrusion detection system, which the study explained to them using Shapley's additional explanation mechanism. The results revealed that the method had high accuracy and F1 value [6]. By integrating secure IoT encryption technology with sensor network security protocol, Mahlake et al. suggested a lightweight security algorithm based on wireless sensor networks to protect IoT data. This algorithm could lower the network's power consumption without compromising network performance. The results indicated that the algorithm key generation time was short [7]. A semi-supervised regularized trapezoidal network-based detection technique was created by Long et al. to identify intrusions in industrial IoT. It achieved this by incorporating streaming regularization restrictions into the trapezoidal network's decoder and taking into account the streaming distribution of high-dimensional (HD) data. By introducing cross-layer connections, it also improved the propagation of inter-layer features. The results revealed that the method had a low false alarm rate [8]. Ahmad et al. designed an intrusion detection algorithm based on particle swarm optimization deep stochastic neural network to develop network security mechanisms through intelligent data processing techniques. The results revealed that the algorithm outperformed other existing models [9]. Latif et al. designed a hybrid model based on artificial neural network and proportional conjugate gradient for improving the cyber security of IoT. It utilized the stochastic paradigm of the artificial neural network process and used the proportional conjugate gradient for learning the weights, and the model's remarkable accuracy was demonstrated by the findings [10].

Liu et al. proposed a ship trajectory prediction framework based on long and short-term memory (LSTM) networks in order to facilitate smart transportation services in maritime IoT. Their modeling of ship traffic conflict scenarios generated using dynamic satellite land data and social force concepts were embedded into a LSTM network and a hybrid loss function was reconstructed. The outcomes revealed the high accuracy and robustness of the method [11]. To address the issue of inadequate security of the current industrial IoT, Li et al. developed a secure routing technique based on multi-objective chaotic elite adaptive ant colony optimization. It initialized the population through a hybrid optimization strategy and dynamically adjusted the algorithm trend using an adaptive optimization strategy [12]. To meet the security requirements of modern IoTs that are unable to provide cross-domain access, Gong et al. suggested a lightweight cross-domain bidirectional authentication technique for mobile IoT environments. The outcomes indicated that the method performed better in terms of computational and communication overheads [13]. The requirement for more precise identification of anomalous traffic in the IoT that deviates from typical traffic patterns prompted Shi et al. to create a deep anomalous network traffic detection model. According to the findings, the model was able to properly account for the specifics of the data distribution [14]. To increase the security of IoT networks, Thota et al. created a botnet detection technique based on enhanced convolutional social networks. The outcomes indicated that the method could effectively detect IoT network intrusion attacks [15].

In summary, although some progress has been made in IoT network security detection in recent years, the existing research still suffers from limited effect in dealing with HD data and low generalization ability of the model. Therefore, the study designs an IoT NSSA method based on improved SVM (ISVM). By introducing radial basis kernel function (KF) for kernel mapping processing of feature vectors (FVs), and to optimize the ISVM parameters, the study proposes a parameter optimization method based on GA-IGWO. It uses GWO algorithm for parameter optimization and introduces circular chaotic mapping and genetic algorithm (GA) for improvement to design an integrated algorithm.

III. ISVM-GA-IGWO Based IoT NSSA Algorithm

This section focuses on the implementation of stochastic nonlinear analysis method for IoT network performance and security. The first section shows the implementation of ISVM based IoT NSSA method. The second section shows the implementation of ISVM parameter optimization method based on GA-IGWO.

A. ISVM-Based IoT NSSA Approach

The secret to ensuring the system operates safely is IoT network security. People's lives are made more convenient by the extensive use of IoT devices in industries such as intelligent transportation, medical and health care, smart homes, and industrial control. However, it also brings new security threats and challenges at the same time, and strengthening the security of IoT networks has become an important task for maintaining social security [16]. However, traditional IoT network security detection often uses rule-based and statistics-based methods. While the data in IoT networks are nonlinearly differentiable, traditional methods cannot effectively deal with this nonlinear relationship. In recent years, the application of DL techniques in IoT network security detection has gradually gained attention. As a powerful supervised learning algorithm, SVM, with its excellent generalization ability and effective handling of nonlinear problems, shows strong application potential in the fields of pattern recognition, classification and regression analysis. Therefore, the study adopts SVM to deal with nonlinearly differentiable data in IoT NSSA. Moreover, the KF of SVM is improved to design an ISVM-based IoT NSSA method. Fig. 1 displays the SVM algorithm's schematic diagram.

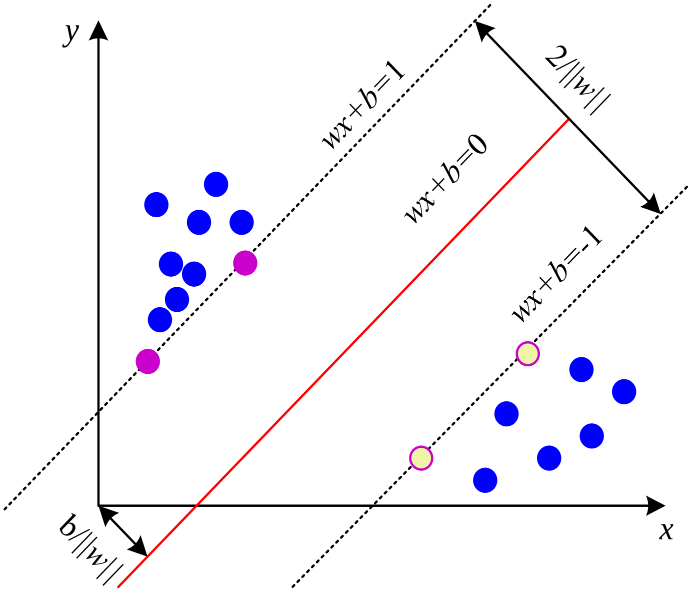


Fig. 1. Principle of SVM algorithm.

The SVM in Fig. 1 seeks to identify a hyperplane that maximizes the category spacing in order to get the best possible classification accuracy. In reality, the hyperplane is a straight line in two dimensions. The objective of SVM classification is to identify a straight line that divides the sample points of various categories and to maximize the distance to the closest point to the straight line. This distance is called the interval, and it needs to be maximized as much as possible during computation. The given hyperplane expression is shown in Eq. (1).

$$H = w^T x + b \tag{1}$$

In Eq. (1), H is hyperplane. w is the weight vector. x is the FV. b is the bias term. T stands for transpose. In order to maximize the interval, for positive class samples (CSs), $w^T x + b \geq 1$ needs to be guaranteed. For negative CSs, $w^T x + b \leq -1$ needs to be guaranteed. Then, the interval can be computed, which is shown in Eq. (2).

$$n = \frac{2}{\|w\|} \tag{2}$$

In Eq. (3), η represents the interval. The next step to maximize the interval is to determine the objective function (OF), which is equivalent to minimizing the square of ‖ w ‖ The calculation is shown in Eq. (3).

$$f_{(n)} = min\frac{1}{2} \parallel w \parallel^2 \tag{3}$$

In Eq. (3), $f(\eta)$ represents the maximum interval. In practical applications, the data are not linearly differentiable. Therefore, soft intervals are introduced to optimize the classification results by allowing classification errors to some extent through slack variables and penalty functions. Eq. (4) displays the expression for OF.

$$f_{(n)} = min\frac{1}{2} \parallel w \parallel^2 + C\sum_{i=1}^{n} \xi_i \tag{4}$$

In Eq. (4), $f'(\eta)$ represents the optimized OF. The OF needs to satisfy the classification constraints and the constraints are shown in Eq. (5).

$$y_i(w^T x_i + b) \geq 1 \tag{5}$$

In Eq. (5), y_i represents class i labeling. The SVM classification is shown in Fig. 2.

Subsequently, the fitness function (FF) is chosen and in the original problem, the optimized variables are weight variables with the same dimensions as the number of features. The Lagrange dyadic function is used in the study to enhance the model's generalization. In the dyadic problem, the optimized variable is the Lagrange multiplier with the same dimension as the number of samples. When the samples' quantity is substantially greater than the number of features, this can greatly lower the computational complexity [17]. The constructed Lagrange dyadic function is displayed in Eq. (6).

$$L(w,b,a) = \frac{1}{2} \parallel w \parallel^2 - \sum_{i-1}^{n} a_i[y_i(w^t x_i + b) - 1 \tag{6}$$

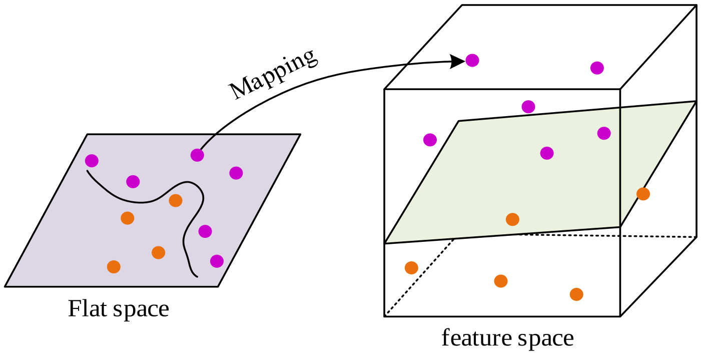


Fig. 2. Feature mapping.

In Eq. (6), α represents the Lagrange multiplier. In dyadic functions, the KF is allowed. Therefore, finally, the study introduces the KF to further optimize the SVM. With the KF, it is possible to compute the inner product directly in the HD space without the need to explicitly perform HD mapping. This allows the SVM to handle nonlinearly differentiable data with the expression shown in Eq. (7).

$$L' = \sum_{i=1}^{n}\alpha_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_j y_i y_j K(x_i,x_j) \tag{7}$$

In Eq. (7), L' represents the OF after introducing the KF, and $K(x_i,x_j)$ represents the KF. So far, the design of ISVM is completed. The flow of ISVM-based IoT NSSA method is shown in Fig. 3.

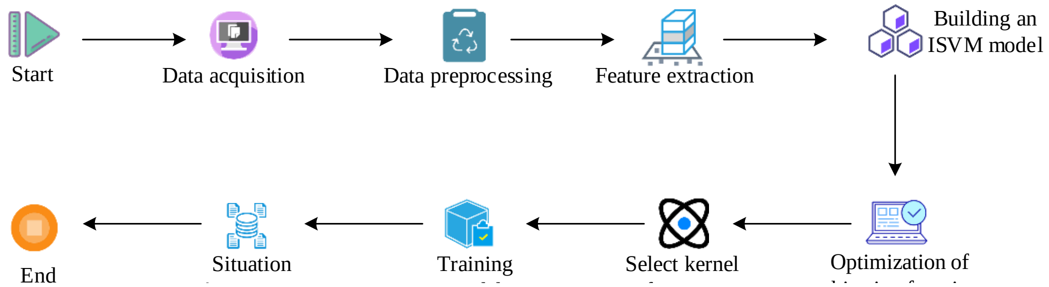


Fig. 3. Process of IoT NSSA method based on ISVM.

B. GA-IGWO-Based Optimization of ISVM Parameters

Even though the suggested NSSA approach for ISVM exhibits great application potential when handling nonlinearly differentiable data, the KF selection and parameter setting have a significant impact on SVM performance. Its selection of parameters and penalty factors for the KF remains challenging. The model may become overfit or underfit as a result of improper parameter selection, which could impair the model's capacity for generalization and classification [18]. Therefore, the study is conducted to optimize the selection of grey wolf (GW) populations through the GWO algorithm for parameter optimization and the introduction of circular chaotic mapping instead of random generation. Meanwhile, GA is introduced to improve the optimized GWO algorithm, and a GA-IGWO-based ISVM parameter optimization method is designed. Fig. 4 displays the schematic diagram of GW hunting activity.

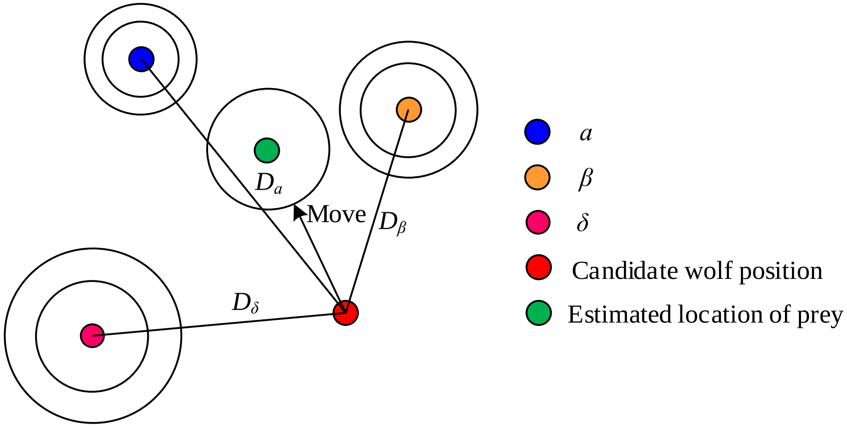


Fig. 4. Schematic diagram of GW hunting behavior.

In Fig. 4, there is a strict hierarchy in the GW group. Among them, α wolf represents the leader in the group, responsible for leading the hunt, corresponding to the optimal solution in the algorithm. The β-wolf is the secondary leader and assists the α-wolf, corresponding to the suboptimal solution. δ wolves are ordinary members that carry out the orders of α and β wolves, corresponding to the third best solution. ω wolves are ordinary members of the pack and follow other wolves in hunting. The GWO algorithm consists of three main hunting behaviors. One is stalking, chasing, and approaching prey, in which the GW searches by dispersing and then focuses on attacking the prey. The second strategy is to harass, encircle, and chase the prey until they cease moving. Attacking the victim while it stops moving is the third tactic [19]. To model the GW's prey encirclement behavior, the expression is calculated as shown in Eq. (8).

$$\begin{cases} D = | C \cdot X_p(t) - X(t) | \\ X(t+1) = X_p(t) - A \cdot D \end{cases} \tag{8}$$

In Eq. (8), D is the relative distance between the current wolf and the target wolf. A and C are the coefficients. X_p is the position of the prey. t is the current iteration quantity. $X(t)$ is the position of the individual GW in the t th generation. Among them, the coefficients A and C are calculated as shown in Eq. (9).

$$\begin{cases} A = 2a \cdot r_1 - a \\ C = 2 \cdot r_2 \end{cases} \tag{9}$$

In Eq. (9), r_1 and r_2 represent random numbers in the interval [0, 1]. a represents the convergence factor. To simulate approaching prey, A is a random number in the interval [$-a$, a]. Over the course of the iteration, the convergence factor drops from 2 to 0. GWs have the ability to recognize the location of prey and round up the prey. Roundups are usually directed by α wolves. β-wolves and δ-wolves also occasionally participate in the hunt [20]. Eq. (10) depicts the mathematical model of a single GW locating the location of prey.

$$\begin{cases} D_\alpha = \left| -X + C_1 \times X_\alpha \right| \\ D_\beta = \left| -X + C_2 \times X_\beta \right| \\ D_\delta = \left| -X + C_3 \times X_\delta \right| \end{cases} \tag{10}$$

In Eq. (10), D_α , D_β , and D_δ display the distance between α -wolf, β -wolf, and δ -wolf and other individuals. X_α, X_β, and X_δ display the current position of α wolf, β wolf, and δ wolf, respectively. C_1, C_2 , and C_3 display random numbers. Subsequently, the adjusted position of the GW can be obtained, which is calculated as shown in Eq. (11).

$$\begin{cases} X_1 = X_\alpha - A_1 \times D_\alpha \\ X_2 = X_\beta - A_2 \times D_\beta \\ X_3 = X_\delta - A_3 \times D_\delta \end{cases} \tag{11}$$

Since in the GWO algorithm, the convergence factor is the variable that mainly affects the breadth and depth search. When it is greater than 1, the GW group will expand the encirclement circle, at this time, the algorithm is mainly breadth search. When it is less than 1, the GW group will narrow the encirclement circle to complete the encirclement attack on the prey. At this time, the algorithm is mainly for the depth search. When the proportion of breadth search in the whole search process is too small, the algorithm will easily fall into the local optimum, and can not find the global optimum point. However, when the proportion of breadth search is too much, it will bring more randomness and uncertainty to the algorithm's optimization process. Therefore, the study introduces circular chaotic mapping to optimize the convergence factor, which is calculated as shown in Eq. (12).

$$\begin{cases} x_{i+1} = \left\{ x_i + r - \dfrac{\sin(2\pi x_i)}{4\pi} \right\} \mathrm{mod}(1) \\ a' = 2(1 - (\dfrac{t}{t_{\max}})^e) \end{cases} \tag{12}$$

In Eq. (12), r represents the constant term, mod represents the summation, and a' represents the improved convergence factor. The flow of the IGWO is shown in Fig. 5.

In the meantime, the study presents GA to optimize the subgeneration population of the GWO algorithm because of its sluggish convergence and susceptibility to local optimization issues. It is necessary to first determine the fitness value (FF) of the j th individual for each member of the GWO subgeneration population. Eq. (13) is used to determine the likelihood that a person will be chosen in a selection.

$$P_j = \frac{F_j}{\sum_{j=1}^{m} F_j} \tag{13}$$

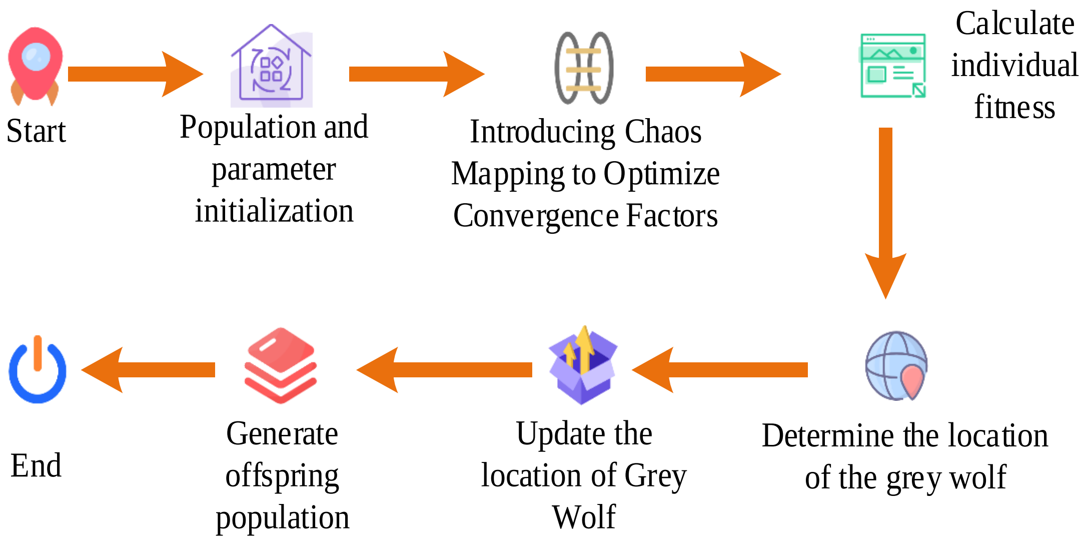

Start
Population and parameter initialization
Introducing Chaos Mapping to Optimize Convergence Factors
Calculate individual fitness
Determine the location of the grey wolf
Update the location of Grey Wolf
Generate offspring population
End

Fig. 5. IGWO process.

In Eq. (13), P_j represents the probability that individual j is selected in a selection. F_j is the FF of the j th individual. Subsequently, a crossover operation is performed to select a cut point in the chromosome. Then, one part of it is exchanged with the corresponding part of the other chromosome to obtain two new individuals. The new individual expression is shown in Eq. (14).

$$\begin{cases} x_{1j}(t)=\frac{1}{2}\times\left[(1-\gamma_j)\mathrm{x}_{2j}(t)+(1+\gamma_j)\mathrm{x}_{1j}(t)\right] \\ x_{2j}(t)=\frac{1}{2}\times\left[(1+\gamma_j)\mathrm{x}_{2j}(t)+(1-\gamma_j)\mathrm{x}_{1j}(t)\right] \end{cases} \tag{14}$$

In Eq. (14), $x_{1j}(t)$ and $x_{2j}(t)$ represent the offspring generated from a pair of parents and the crossover operator. The next step is the mutation operation, which creates a new individual by substituting different alleles for gene values at specific loci in the coding strings of the individual chromosomes. For each locus g_j, the range of continuous uniform distribution of the mutation is determined with the mutation probability. A random perturbation is added to its value to generate a new individual. The calculation is shown in Eq. (15).

$$g'_j = g_j + \delta \tag{15}$$

In Eq. (15), g'_j represents the mutated locus. δ represents the random perturbation drawn from the uniform distribution. Finally, the mean absolute percentage error (MAPE) is used to construct the FF to calculate the FF and the optimal parameters. The FF is shown in Eq. (16).

$$f(y)=\frac{1}{1+MAPE(y)} \tag{16}$$

In Eq. (15), y represents the optimal parameters and $MAPE$ represents MAPE. The flow of GA-IGWO is shown in Fig. 6.

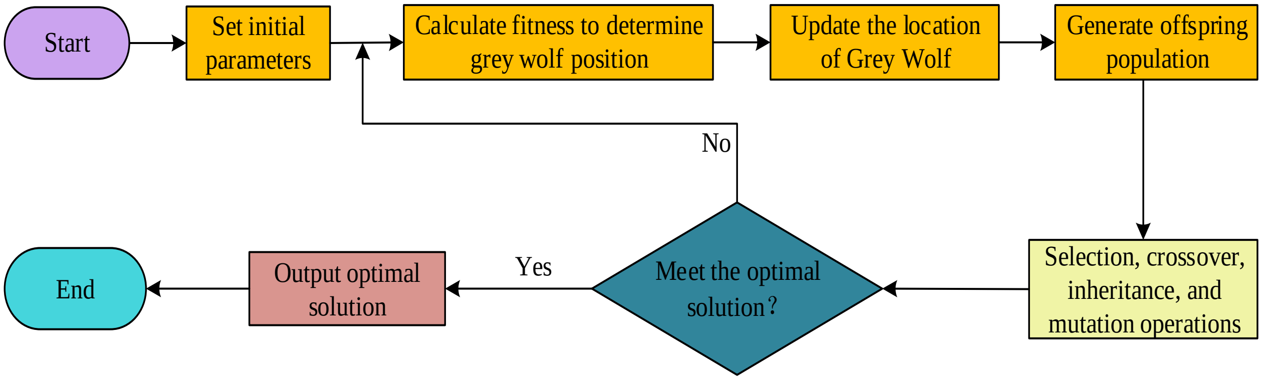

Start
Set initial parameters
Calculate fitness to determine grey wolf position
Update the location of Grey Wolf
Generate offspring population
No
Selection, crossover, inheritance, and mutation operations
Meet the optimal solution？
Yes
Output optimal solution
End

Fig. 6. GA-IGWO flow.

IV. Effectiveness Analysis of ISVM-GA-IGWO-Based IoT NSSA Algorithm

This section deals with the effectiveness analysis of ISVM-GA-IGWO-based IoT NSSA algorithm. The first section shows the performance analysis results of ISVM-GA-IGWO based IoT NSSA algorithm. The second section shows the results of practical application effect of ISVM-GA-IGWO NSSA algorithm.

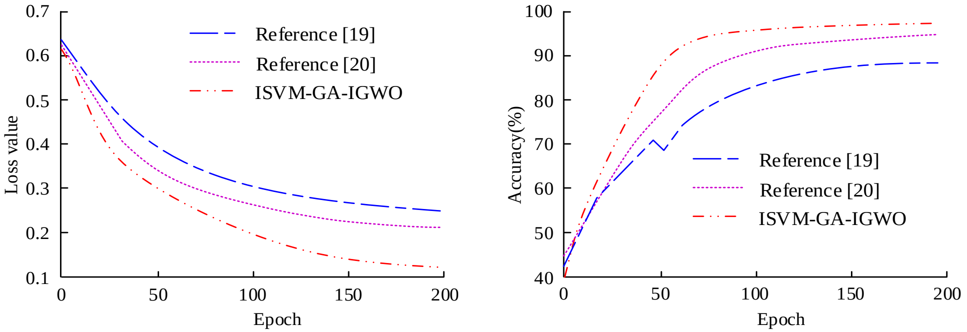
A. *Performance Analysis of ISVM-GA-IGWO NSSA Algorithm*

To validate the performance of ISVM-GA-GWO-based IoT NSSA algorithm, the study is carried out on an operating system equipped with Intel core i7-11390H central processor, 32 GB of running memory, 32 GB of video card memory and Windows 11. The simulation is also analyzed using Python 3.7. The maximum iteration of the ISVM-GA-GWO algorithm is firstly set to 200, the population size is set to 50, the crossover operator is 0.7, and the variation operator is 0.02. The accuracy of ISVM-GA-GWO is firstly verified by introducing mean absolute error (MAE), root mean square error (RMSE), and MAPE. It is also compared with SVM, and GWO, methods in [19] and [20]. Table I displays the findings.

TABLE I TRAINING PARAMETERS OF THE MODEL

Model	MSE	RMSE	MAPE
SVM	0.0213	0.125	0.0032
GWO	0.0142	0.114	0.0053
Reference [19]	0.0112	0.092	0.0026
Reference [20]	0.0089	0.074	0.0021
ISVM-GA-IGWO	0.0064	0.041	0.0013

In Table I, the MAE, RMSE, and MAPE of ISVM-GA-IGWO are 0.0064, 0.041, and 0.0013, respectively. The MSEs of [20], [19], GWO, and SVM are 0.0089, 0.0112, 0.0142, and 0.0213, respectively. Their RMSE is 0.074, 0.092, 0.114, 0.125, and MAPE is 0.0021, 0.0026, 0.0053, 0.0032, respectively. It can be found that the values of the three indexes of ISVM-GA-IGWO are significantly lower than those of other algorithms, which proves that it is more accurate. To further verify the accuracy of ISVM-GA-IGWO, the study calculates the loss and accuracy of different models separately and compares them with other algorithms. The results are shown in Fig. 7.



(a) Changes in the loss function values of each algorithm

(b) Changes in accuracy of each algorithm

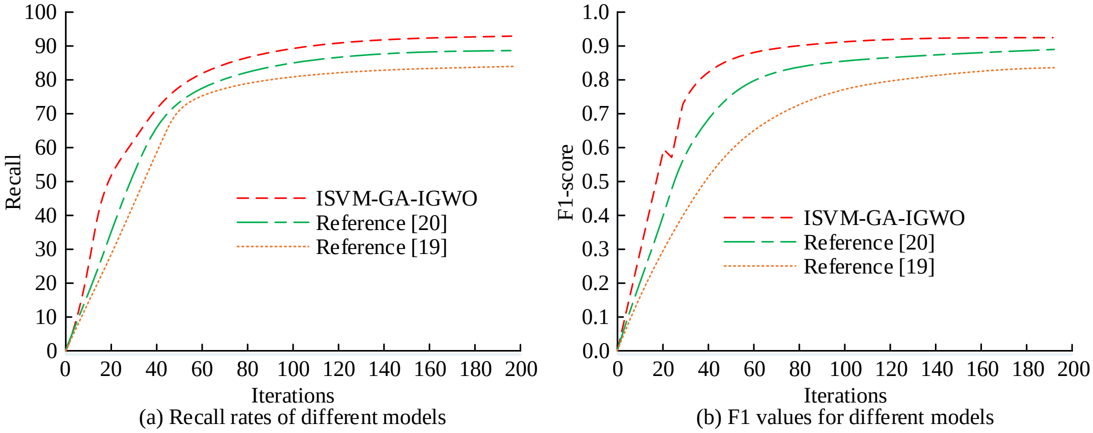
Fig. 7. Value of loss function and accuracy of each algorithm.

In Fig. 7(a), the loss of the algorithm in [19] is 0.25, the loss of the algorithm in [20] is 0.21, and the loss of the proposed ISVM-GA-IGWO is 0.13. The three algorithms have corresponding accuracy rates of 89.2%, 95.6%, and 98.1% in Fig. 7(b). Its superior accuracy is further demonstrated by the fact that ISVM-GA-IGWO has a smaller loss and a greater accuracy rate than the other two algorithms. To provide further validation of the performance of the proposed IoT network security situation assessment algorithm based on ISVM-GA-GWO, five indicators, including area under curve (AUC), memory usage, throughput, average detection time, and false alarm rate, are introduced to calculate the non-algorithmic indicator values. The comparison results are shown in Table II.

In Table II, the AUC, memory usage, throughput, average detection time, and false positive rate of the SVM algorithm are 0.855, 483 MB, 74.8 Mbps, 5.1 s, and 14.6%, respectively. The five indicators of GWO are 0.887, 412 MB, 78.5 Mbps, 4.3 s, and 11.2%, respectively. The five indicator values of SVM-GA-GWO are 0.923, 356 MB, 82.1 Mbps, 3.8 s, and 9.1%, respectively. The five indicator values of the algorithm in [19] are 0.946, 328 MB, 85.6 Mbps, 3.5 s, and 8.5%, respectively. The five indicator values of the algorithm in [20] are 0.952, 289 MB, 91.2 Mbps, 2.7 s, and 5.3%, respectively. The five indicators of the ISVM-GA-IGWO algorithm are 0.981, 224 MB, 97.3 Mbps, 1.2 s, and 2.2%, respectively. It can be observed that compared to other algorithms, the proposed ISVM-GA-IGWO algorithm has significantly higher AUC values and throughput, with a maximum AUC increase of 0.126 and a maximum throughput increase of 22.5 MB. However, a marked decline in memory usage, average detection time, and false alarm rate has been observed. Specifically, the memory usage can be reduced by up to 259 Mbps, the average detection time can be reduced by up to 3.9 s, and the false alarm rate can be reduced by up to 12.4%. The aforementioned results demonstrate that the proposed IoT network security situation assessment algorithm based on ISVM-GA-GWO performs well in terms of detection accuracy, real-time performance, and resource utilization. Lastly, the algorithm in [20], ISVM-GA-IGWO, and the algorithm in [19] are evaluated for recall and F1 value. Fig. 8 displays the findings.

TABLE II COMPARISON OF INDICATOR VALUES FOR DIFFERENT ALGORITHMS

Model	AUC	Memory usage (MB)	Throughput (Mbps)	Mean time to detect (s)	False alarm rate (%)
SVM	0.855	483	74.8	5.1	14.6
GWO	0.887	412	78.5	4.3	11.2
SVM-GA-GWO	0.923	356	82.1	3.8	9.1
Reference [19]	0.946	328	85.6	3.5	8.5
Reference [20]	0.952	289	91.2	2.7	5.3
ISVM-GA-IGWO	0.981	224	97.3	1.2	2.2



(a) Recall rates of different models

(b) F1 values for different models

Fig. 8. Recall rates and F1 values of different models.

Fig. 8(a) illustrates the recall of the three algorithms. The recall of ISVM-GA-IGWO is 93.7%, the recall of the model in [20] is 89.3%, and the recall of the model in [19] is 83.6%. Fig. 8(b) demonstrates the F1 value of the three algorithms. The F1 value of the three algorithms is 0.94, 0.90, and 0.84, respectively. The suggested ISVM-GA-IGWO method provides a recall rate that is 4.4% and 10.1% greater than the algorithms in [19] and [20], and its F1 value is 0.04 and 0.10 higher than those of the other two algorithms, respectively. It shows that ISVM-GA-IGWO has better overall performance.

B. *Analysis of the Effect of Practical Application of ISVM-GA-IGWO NSSA Algorithm*

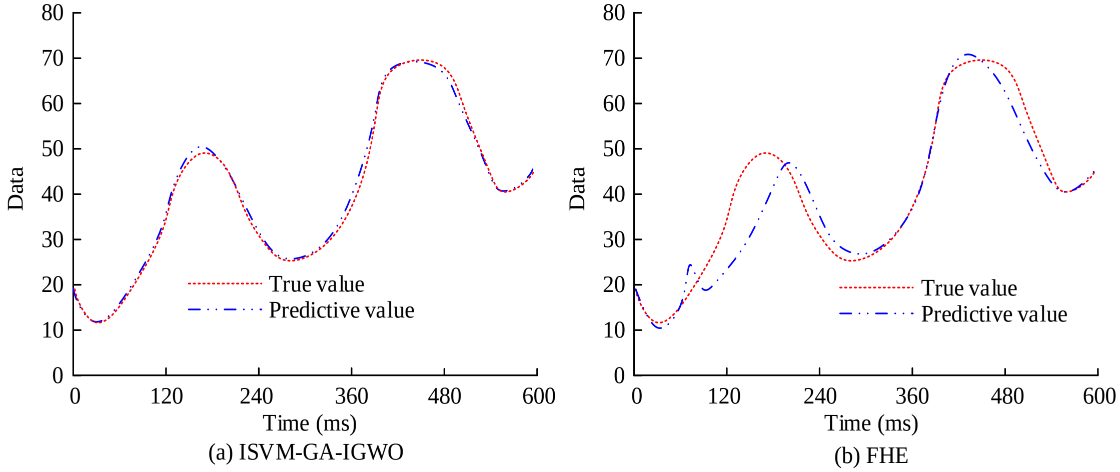
To verify the practical application of the designed ISVM-GA-IGWO based IoT NSSA algorithm, the study firstly validates the ISVM-GA-IGWO model in five aspects, namely, whether it supports attribute revocation, offline encryption, outsourcing decryption, authorization center, and key length. The support is denoted as T and not as F. The unit key length is denoted by L and compared with the other two algorithms. Table III displays the findings.

In Table III, for the first four aspects, ISVM-GA-IGWO performs T. The ABE algorithm performs T in three aspects: attribute revocation, offline encryption, and outsourcing decryption. It performs F in authorization centers. The FHE algorithm performs the same way as the ABE algorithm in the four aspects. The key length L+1 of ISVM-GA-IGWO is smaller than ABE algorithm and FHE algorithm. The above outcomes indicate that the ISVM-GA-IGWO is more powerful. The next step is to calculate the data access control effect of different algorithms within 600 ms respectively. The results are shown in Fig. 9.

In Fig. 9, when access control is performed by the ISVM-GA-IGWO, the predicted curves largely coincide with the actual curves. When access control is performed using the FHE algorithm, the predicted curves deviate significantly from the actual curves around 120 ms and 480 ms. It indicates that the ISVM-GA-IGWO fitting performance is better and works better in practical applications. Next, the overhead and time during communication is calculated and the results are compared with other algorithms as shown in Fig. 10.

TABLE III FUNCTIONAL COMPARISON OF DIFFERENT ALGORITHMS

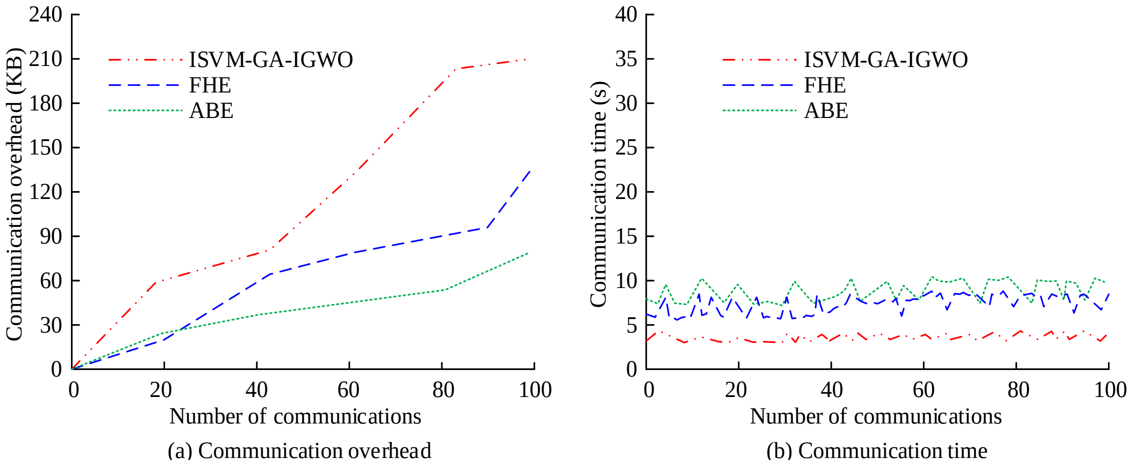
Algorithm	ABE	FHE	ISVM-GA-IGWO
Access structure	F	F	T
Offline encryption	F	F	T
Outsourced encryption	F	F	T
Authority center	T	T	T
Key length	2L+4	2L+1	L+1



(a) ISVM-GA-IGWO

(b) FHE

Fig. 9. Data processing capacity of different algorithms within 1000 ms.



(a) Communication overhead

(b) Communication time

Fig. 10. Communication overhead between different decryption algorithms is sent to data centers and sent to data receivers.

In Fig. 10(a), the communication overheads of the different algorithms all show an increasing trend as the communication increases. When the communication reaches 100 times, the communication overhead of ISVM-GA-IGWO is 81.3 KB, which is significantly lower than 134.6 KB of FHE algorithm and 211.5 KB of ABE algorithm. In Fig. 10(b), the average communication time of ABE algorithm, FHE algorithm, and ISVM-GA-IGWO is 8.11 s, 6.37 s, and 3.59 s. The average communication time of ISVM-GA-IGWO is significantly lower than the other methods. The above outcomes display that the ISVM-GA-IGWO can effectively reduce the communication cost and delay, which further proves that its practical application is more effective. To verify the effectiveness of the proposed ISVM-GA-IGWO network security situation assessment algorithm in practical applications, the proposed method is validated in several scenarios. These scenarios include an intelligent furniture network containing 50 smart devices, an industrial control system based on Modbus protocol, intelligent urban traffic monitoring deployed on traffic signal lights and camera networks, a medical IoT with electrocardiogram monitors and insulin pump devices, and a vehicle-to-infrastructure communication simulation. The results are shown in Table IV.

TABLE IV EVALUATION RESULTS OF ISVM-GA-IGWO ALGORITHM IN DIFFERENT SCENARIOS

Test scenario	**Anomaly detection rate (%)**	**False positive rate (%)**	**Average response time (s)**	**Communication overhead (KB)**
Smart home network	96.2	1.3	5.8	82.1
Industrial control system	94.8	0.9	7.2	85.7
Smart city traffic monitoring	97.5	1.1	6.4	78.9
Medical Internet of Things	95.1	0.7	8.1	90.3
Internet of Vehicles	93.6	1.5	9.5	102.5

As illustrated in Table IV, the proposed ISVM-GA-IGWO network security situation assessment algorithm demonstrates a noteworthy performance in terms of anomaly detection, with a rate of 96.2%. The algorithm exhibits a low false alarm rate of 1.3%, an average response time of 5.8 seconds, and a communication overhead of 82.1 KB. In industrial control systems, smart city traffic monitoring, medical IoT, and vehicle networking, the proposed algorithms have anomaly detection rates of 94.8%, 97.5%, 95.1%, and 93.6%, and false alarm rates of 0.9%, 1.1%, 0.7%, and 1.5%, respectively. The average response times are 7.2 s, 6.4 s, 8.1 s, and 9.5 s, respectively, and the communication overheads are 85.7 KB, 78.9 KB, 90.3 KB, and 102.5 KB, respectively. It has been demonstrated that, under various conditions, the algorithm exhibits a high capability for anomaly detection and a low rate of false alarms, while maintaining minimal response time and communication overhead. These observations suggest that the proposed ISVM-GA-IGWO network security situation assessment algorithm is well-suited to meet the stringent requirements of precision and real-time performance in practical scenarios.

V. Discussion

The research aimed to solve the problem of poor performance of traditional IoT network performance analysis methods in handling random nonlinear features, and proposed a network security situation assessment method based on ISVM-GA-IGWO. The MAE value of this method was 0.0064, the RMSE value was 0.041, and the MAPE value was 0.0013, which were significantly lower than other algorithms, indicating its high prediction accuracy. This was similar to the conclusion of Thota S et al [15]. In contrast, ISVM-GA-IGWO was significantly better because the GA-IGWO optimization resulted in better parameters, allowing the model to better fit complex data. The F1 value of the ISVM-GA-IGWO algorithm was 0.94, with a recall rate of 93.7%, indicating its good overall performance. This was consistent with the conclusion drawn by Oseni et al. [6], but the ISVM-GA-IGWO algorithm performed better. This was because the proposed algorithm introduced GWO and optimized it by circular chaotic mapping. At the same time, it introduced radial basis KFs to perform kernel mapping on FVs, which significantly improved the performance. The memory usage of the ISVM-GA-IGWO algorithm was only 224 MB, which proved its good resource utilization. This result was similar to the conclusion of Shi G [14]. Compared with these two methods, the proposed method was obviously better. Because, in the optimization process of ISVM-GA-IGWO algorithm, the method avoided redundant parameter storage and complex computation process by reasonably setting the population size, optimizing the genetic operation, and simplifying the design of ISVM model, which effectively reduced the memory overhead. In summary, the ISVM-GA-IGWO algorithm proposed in this study demonstrates significant advantages in the field of IoT network security situation assessment, providing technical support for the application of IoT in more complex scenarios.

VI. Conclusion

With the surge in the number of IoT devices, the complexity and uncertainty of network traffic have increased significantly, and the cyber security threats have become increasingly severe. Traditional cyber security detection methods, such as rule-based and statistical approaches, have been difficult to cope with the nonlinearly differentiable data and dynamically changing network environment in the IoT environment. The research aimed to address the shortcomings of traditional methods in dealing with nonlinearly differentiable data and to improve the robustness of the model in the face of new attack types and unknown data. It proposed an ISVM-based IoT NSSA method and optimized the parameters of ISVM by combining GA and IGWO. The results revealed that the MAE, RMSE, and MAPE of ISVM-GA-IGWO were 0.0064, 0.041, and 0.0013, respectively. Compared to the values of the three indexes of the four algorithms in [20], [19], GWO, and SVM, it was much lower, demonstrating its great accuracy. ISVM-GA-IGWO had a loss of 0.13 and an accuracy of 98.1%, which was lower than the other methods and higher than the other methods, further proving its higher accuracy. When access control was performed by ISVM-GA-IGWO, the predicted curve basically overlapped with the actual curve. When using the FHE algorithm for access control, the prediction curves had large deviations from the actual curves around 120 ms and 480 ms, indicating that the ISVM-GA-IGWO was more effective in practical application. However, despite the introduction of GA-IGWO algorithm for parameter optimization, it may still fall into local optima in some cases, resulting in unsatisfactory optimization results. At the same time, the proposed ISVM-GA-IGWO hybrid algorithm increases the resource consumption to a certain extent, and the model performance is highly dependent on high-quality annotated data, while in actual IoT environments, abnormal samples are rare and annotation costs are high. In addition, the device state and network topology in IoT may change frequently, and the current model lacks adaptability to dynamic environments. Subsequent research endeavors will introduce more efficient parameter optimization algorithms, such as adaptive parameter control or dynamic weight adjustment, to enhance the convergence speed and robustness of the model. Meanwhile, multi-objective optimization methods will be explored to simultaneously optimize multiple performance indicators. In addition, semi- or self-supervised learning will be combined to reduce the dependence on annotated data, and online learning or incremental update mechanisms will be added to adapt to dynamic scenarios.

References

[1] M. M. Khayyat, S. Abdel-Khalek, R. F. Mansour. "Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment," Alex Eng J, Vol. 61, No. 12, pp. 11377-11389, May 2022.

[2] M. Srinivasulu, G. Shivamurthy, B. Venkataramana. "Quality of service aware energy efficient multipath routing protocol for internet of things using hybrid optimization algorithm," Multimed Tools Appl, Vol. 82, No. 17, pp. 26829-26858, April 2023.

[3] D. Jiang, Z. T. Njitacke, J. D. D. Nkapkop, N. Tsafack, X. Wang, J. Awrejcewicz. "A new cross ring neural network: Dynamic investigations and application to WBAN," IEEE Internet Things, Vol. 10, No. 8, pp. 7143-7152, December 2022.

[4] A. Heidari and M. A. Jabraeil Jamali. "Internet of Things intrusion detection systems: a comprehensive review and future directions," Cluster Comput, Vol. 26, No. 6, pp. 3753-3780, October 2023.

[5] V. Gugueoth, S. Safavat, and S. Shetty. "Security of Internet of Things (IoT) using federated learning and deep learning—Recent advancements, issues and prospects," ICT Express, Vol. 9, No. 5, pp. 941-960, October 2023.

[6] A. Oseni, N. Moustafa, G. Creech, N. Sohrabi, A. Strelzoff, Z. Tari, and I. Linkov. "An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks," IEEE T Intell Transp, Vol. 24, No. 1, pp. 1000-1014, July 2022.

[7] N. Mahlake, T. E. Mathonsi, D. Du Plessis, and T. Muchenje. "A lightweight encryption algorithm to enhance wireless sensor network security on the Internet of Things," J Commun, Vol. 18, No. 1, pp. 47-57, January 2023.

[8] J. Long, W. Liang, K. C. Li, J. Long, W. Liang, K. C. Li, Y. Wei, and M. D. Marino. "A regularized cross-layer ladder network for intrusion detection in industrial internet of things," IEEE T Ind Inform, Vol. 19, No. 2, pp. 1747-1755, September 2022.

[9] J. Ahmad, S. A. Shah, S. Latif, F. Ahmed, Z. Zou, N. Pitropakis. "DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things," J King Saud Univ-Com, Vol. 34, No. 10, pp. 8112-8121, November 2022.

[10] S. Latif, Z. Sabir, M. A. Z. Raja, G. C. Altamirano, R. A. S. Núñez, D. O. Gago, and M. R. Ali. "IoT technology enabled stochastic computing paradigm for numerical simulation of heterogeneous mosquito model," Multimed Tools AppL, Vol. 82, No. 12, pp. 18851-18866, December 2023.

[11] R. W. Liu, M. Liang, J. Nie, W. Y. B. Lim, Y. Zhang, and M. Guizani. "Deep learning-powered vessel trajectory prediction for improving smart traffic services in maritime Internet of Things," IEEE T Netw Sci Eng, Vol. 9, No. 5, pp. 3080-3094, January 2022.

[12] C. Li, Y. Liu, J. Xiao, and J. Zhou. "MCEAACO-QSRP: A novel QoS-secure routing protocol for industrial Internet of Things," IEEE Internet Things, Vol. 9, No. 19, pp. 18760-18777, March 2022.

[13] B. Gong, G. Zheng, M. Waqas, S. Tu, and S. Chen. "LCDMA: Lightweight cross-domain mutual identity authentication scheme for Internet of Things," IEEE Internet Things, Vol. 10, No. 14, pp. 12590-12602, March 2023.

[14] G. Shi, X. Shen, F. Xiao, and Y. He. "DANTD: A deep abnormal network traffic detection model for security of industrial internet of things using high-order features," IEEE Internet Things, Vol. 10, No. 24, pp. 21143-21153, March 2023.

[15] S. Thota and D. Menaka. "Botnet detection in the internet-of-things networks using convolutional neural network with pelican optimization algorithm," Automatika, Vol. 65, No. 1, pp. 250-260, December 2024.

[16] M. Mir, M. Yaghoobi, and M. Khairabadi. "A new approach to energy-aware routing in the Internet of Things using improved Grasshopper Metaheuristic Algorithm with Chaos theory and Fuzzy Logic," Multimed Tools Appl, Vol. 82, No. 4, pp. 5133-5159, January 2023.

[17] S. N. G. Aryavalli and G. H. Kumar. "Futuristic vigilance: Empowering chipko movement with cyber-savvy IoT to safeguard forests," Archives of Advanced Engineering Science, Vol. 2, No. 4, pp. 215-223, September 2024.

[18] A. Yazdinejad, M. Kazemi, R. M. Parizi, and R. M. Parizi. "An ensemble deep learning model for cyber threat hunting in industrial internet of things," Digit Commun Netw, Vol. 9, No. 1, pp. 101-110, February 2023.

[19] L. A. Maghrabi, S. Shabanah, T. Althaqafi, D. Alsalman, S. Algarni, A. A. M. Al-Ghamdi, and M. Ragab. "Enhancing cyber security in the internet of things environment using bald eagle search optimization with hybrid deep learning," IEEE Access, Vol. 12, pp. 8337-8345, January 2024.

[20] R. Fu, X. Ren, Y. Li, Y. Wu, H. Sun, and M. A. Al-Absi. "Machine-learning-based UAV-assisted agricultural information security architecture and intrusion detection," IEEE Internet Things, Vol. 10, No. 21, pp. 18589-18598, November 2023.