Received: May 8, 2025. Revised: May 31, 2025.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Dynamic Parameter Optimization for Industrial Internet Security Models Using Neural Networks

Darun Mudhafar Hamad [1] Wisam Hazim Gwad[2] Wafa Hussain Fadaaq[3]
Shahab Wahhab Kareem[4,5]*

[1]*Department of Computer Science, College of Computer Science and Information Technology, Catholic University in Erbil, Erbil, KR, Iraq*
[2]*Department of Artificial Intelligence Engineering, College of Engineering. Alnoor University, Ninavah, Iraq*
[3]*Department of Information Technology &Computer Science at Stardom University, Istanbul, Turkey*
[4]*Department of Technical Information Systems Engineering, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq*
[5]*Department of Computer Technical Engineering, Al-Qalam University College, Kirkuk, Iraq*
* Corresponding author's Email: shahab.kareem@epu.edu.iq

Abstract: The Industrial Internet of Things, or IIoT, transforms industries by allowing complex systems to interact with each other, but opens up industries to new and more advanced threats, including DDoS attacks, ransomware, and malware. These current security models for IIoT inherently use static optimization approaches that do not match real-time changes and other attack patterns. To overcome these limitations, this study calls for developing the Dynamic Parameter Optimization Framework that will incorporate the use of both the Neural Network and Black Winged Kite Algorithm (BKA) to optimize a given process in real time. The framework incorporates several models: XGBoost, a spatial CNN particularly designed using PSO with Default, and a BKA for tuning the CNN for dynamic parameters. Thus, the proposed method, which balances the exploration and exploitation capabilities of BKA optimizes such variables like learning rates and weights well. Moreover, Proposed mechanisms make consideration of changes in threats, as well as a large-scale IIoT environment, possible. The evaluations of TON_IoT and UNSW-NB15 datasets presented the framework's efficiency, where the accuracy achieved 96.8% and F1-score of 95.3%, outperforming the Particle Swarm Optimization (PSO) and XGBoost methods. The framework also provided a 20% improvement in convergence time and adaptation capability by updating the parameters in real-time. This study provides a foundation to develop a sound, elastically adaptive, and autonomously executable security framework for IIoT that calls for minimal human intervention to tackle cyber threats. Future work plans to develop this framework to work with multi-modal data and to perform well in various industrial environments.

Keywords: Dynamic parameter optimization, Industrial internet of things (IIoT), Convolution neural networks (CNN), Black-winged kite algorithm (BKA).

1. Introduction

IIoT is the advanced level of IoT that nowadays has changed industries as interconnected devices and systems improve the efficiency, automation, and decision-making processes of them. However, depending on the internet, these new systems of IIoT have attracted several cyber risks which include the DDoS attacks, ransomware, and malware intrusions. These threats are dangerous to industrial control systems that are crucial in determining operational security and productivity. Typical methods of security assessment are static and do not allow for timely evaluation of emerging threats which create weak links in industrial networks [1]. The development of more advanced machine learning as well as artificial intelligence provides hope to offer security solutions for IIoT systems. Of the discussed techniques, the most successful have been neural networks in the areas of intrusion detection,

anomalies, and parameter tuning. For instance, deep random neural networks or ensemble learning models are suitable for detecting cyberattacks in IIoT networks with high accuracy [2]. Nevertheless, there is a necessity to create more sophisticated models to manage security parameters depending on the increased level of industrial network complexity. Although the security advancements achieved in the domain of IIoT, numerous current models depend on metaheuristic algorithms or a set of rules provided by experts, where the adaptability of the optimization approaches is not optimized. The generally employed for parameter optimization in human security models, has issues in giving with the non-stationary and non-linear security parameters [3]. In addition, such methods seem to rely strongly on knowledge from experts in the respective fields and can therefore end up being biases or inaccurate. The use of neural networks as a solution to incorporate them into the security assessment frameworks is possible due to dynamic and automated parameter optimization. Neural networks have the flexibility in the learning of the interconnectivity of security parameters, flexibility in the recognition of change in conditions, and the advantage of the least use of manual tuning. To that end, this paper seeks to strengthen and optimize the security models that advance IIoT through the application of neural networks.

Current security assessment models for IIoT face several challenges:

- Static Optimization Methods: Algorithms such as the S-CMA-ES do not possess the provision of evolving in response to changes in the kind of attacks being executed or changes within the systems[3].
- Heavy Dependence on Expert Knowledge: Configuration of the security parameters can be a cumbersome process and is also prone to errors [4].
- Insufficient Scalability: Traditional models fail to cope with IIoT network size and complexity as the size of the network increases [5].
- Limited Real-Time Capabilities: Currently available solutions are not capable of offering good real-time threat identification and management because of efficiency problems [6].

These limitations suggest the necessity of a new approach that combines the IIoT forensic intent of neural networks with the adaptability of security parameters inside these environments. The solutions used for IIoT cybersecurity in industries are limited in dealing with unexpected and updated attacks. Many of the optimization models available today are static, meaning they use techniques such as PSO and S-CMA-ES which were created for problems that do not change. Because of this, they cannot respond well to new challenges or shifts in the IT environment. Also, setting up traditional security solutions can be slow and requires an expert to manually adjust the key parameters. Additionally, these models are less efficient on computers and cannot continue retraining themselves to use updated information. For this reason, models could be less reliable with new threats, are sometimes unable to detect them and do not scale effectively to a wide variety of industrial systems. Contrarily, this model applies dynamic parameter optimization by combining a CNN and the BKA, along with a learning method. Combining these technologies allows the system to adjust itself, update model settings and retain high accuracy when dealing with sudden changes in the Internet of Things. It means security systems are now being designed to fit the challenges found in today's complex industries.

This paper proposes a Dynamic Parameter Optimization Framework that integrates neural networks into the security assessment of IIoT systems. The key contributions of this research are:

- Neural Network-Based Parameter Optimization: A Convolution neural network model that dynamically learns and optimizes parameters such as rule weights, confidence levels, and utility scores.
- Real-Time Adaptability: Enabling real-time optimization of security parameters to handle evolving threats effectively.
- Reduction in Expert Dependency: Minimizing reliance on manual configuration by utilizing automated learning techniques.
- Improved Scalability and Accuracy: Demonstrating the enhanced performance of the proposed model on large-scale industrial datasets such as TON_IoT and UNSW-NB15.

The proposed framework encounters several challenges:

- Data Diversity: Checking its performance for its ability to generalize other types of IIoT datasets with different attacks.
- Model Complexity: Making a balance between model accuracy and time that it takes to produce the model's result, while still being in real time.
- Integration with Existing Systems: The absence of interruption of services prevalent during integration of standard security elements into IIoT networks / systems.
- Handling Data Imbalance: To overcome the class imbalance problem, which is commonly seen in intrusion detection datasets, and impacts the model.

The remainder of this paper is organized as follows: Section 2 enlists several similar studies and models of IIoT and its security optimization. Section 3: In the case of Methodology, the paper presents the general structure of the framework based on the neural network for the optimization of the parameter and the overall process of integrating the framework into a real-world setting. This work also outlines the datasets used in the validation of the model, the evaluation criteria employed and the experiment settings. Section 4: Results and Discussion discusses the performance comparison of the proposed model with other techniques. Finally, the paper highlights the areas of improvement that can be incorporated into the current work. Section 5: Conclusion and Future Work highlights the findings of the paper and discusses further research areas.

2. Literature review

Various well-known optimization techniques for IIoT security have been suggested, but each of these has flaws when used in changing industrial conditions. For instance, even though PSO is popular for adjusting neural networks, it is noticed that it may result in early solutions and has difficulties exploring options in large or changing environments. Although PSO provides fast solutions at first, it is not strong enough to keep adapting in quick-changing threats. Similar to other approaches, S-CMA-ES delivers satisfactory results in test conditions but does not work well when things are not predictable. Its price in computational resources is significant and it depends a lot on how hyperparameters are set—which must be set up manually. Due to these limitations, S-CMA-ES cannot be applied to IIoT systems that require fast, automatic reactions. In addition, using rules and manual tuning in many industrial security models causes scalability problems and relies on people with specialized knowledge, making them likely to fail when handling unseen types of attacks. Unlike other techniques, our suggested model works by using the Black-Winged Kite Algorithm which employs a unique method to adjust the optimal parameters of neural networks on the fly. We also incorporate a learning process that makes it possible for our model to change over time from newly received IoT data. The use of both strategies makes the overall system flexible and strong, overcoming the issues seen in traditional and semi-automated optimization techniques. In [1] discuss new approaches in machine learning for DDoS detection in IIoT. It focuses on the ability to change the control algorithm at a fine temporal resolution, low computational complexity, and the possibility of its application in large-scale industrial processes. In this paper, classifying and clustering methods are identified as suitable means of dealing with DDoS. The authors present the DRANN_PSO [2], which is a model integrating deep random neural networks with particle swarm optimization in an IIoT intrusion detection context. The model shows the higher accuracy of results and the time required to achieve these results compared to the traditional methods. It is used most efficiently when it targets certain attack patterns that are inherent in IIoT. In [3] generalize how to adjust the neural network for attack detection in the IIoT setting. He proposes ways in which detection accuracy can be improved with the use of learned models and the regulation of the model parameters. The work gives helpful information on dynamic security for industrial systems. The work [4] combines deep belief networks with the convolutional neural network to design a cyberattack detection system for IIoT. It works at multiple layers and is particularly proficient at the identification of various attack patterns. It also points to the fact that there should be strong multilayer learning in IIoT cybersecurity. In [5], the authors present the concept of AFFL, a technique that combines adaptive federated learning and a digital twin for IIoT systems. The approach guarantees secure learning cooperation on distributed systems. It also uses digital twins in accurately model and judging the improvised scenarios of IIoT security. In [6] paper introduces multiple botnet detection ensemble transfer learning models in the IoT network. Algorithms are also investigated for coping with data heterogeneity and imbalance by the authors. According to their model, they portray good adaptability and especially perform well when scenarios of IoT are complex and mixed. The work [7] employs the Recurrent Neural Networks (RNN) for the online detection of malware operating in IoT environments. It stresses on high accuracy and the latency of detection. In terms of their ability to process sequential data, the research finds that RNNs are useful in cybersecurity applications. [8] discusses the use of the deep reinforcement learning approach to IIoT security. New attack strategies are countered by fixed and dynamic response patterns from DRL agents, making the system more robust. In dynamics of threat scenarios, the authors pay special attention to the prospects of autonomous learning. The authors in [9] developed a recurrent neural network-based architecture for secure communication of data through IIoT systems. It expands the protection of data confidentiality and data integrity. A well-documented example in which it is especially useful for shielding confidential industry messages is in its

practical application. In [10] The study proposes and explores a deep random neural network – a deep learning network – for recognizing cyberattacks in IIoT systems. The proposed model successfully detects all the considered attack categories to ensure reliable protection. In addition, some background applied in the experimentation increases the false rate, making the outcomes more reliable in industrial usage. The authors [11] propose a framework for the security of the IIoT networks by combining deep learning with a metaheuristic method for feature selection. The model fixes the shortcomings of detecting anomalies in industrial control systems and improves the accuracy of the results. It also meets the main problems regarding data diversity and scalability. In [12] a deep learning IDS was implemented with rule-based feature selection introduced into it. The approach enhances the model interpretation and its execution or performance aspect. The work [13] presents a Latent Perturbed Neural Network for multi-user physical-layer authentication In IIoT. High authentication accuracy can also be achieved with a relatively low computational cost thanks to the model. What is stressed here is the requirement of a lightweight security solution for industrial premises. The authors [14] develop a two-pathway convolutional neural network that incorporates a spider monkey optimization process for threat identification in cybersecurity. Here the work of the model is best seen when it comes to details of the attack freedom. This shows that the model has high sensitivity with few false positive incidences. [15] focuses on discussing metaheuristic feature selection with deep learning for anomaly detection in IIoT environments. The technique enhances the detection precision and the rate at which the approach operates. It can be used for real-time analysis in and engineering and manufacturing industries. The work [16] proposes synaptic intelligent convolutional neural networks for anomaly detection in the dynamic IoT context. The model performs well when operating in a dynamic network environment. It also focuses on applying Convolutional structures to secure IIoT.

In [17], a lightweight random neural network for IIoT-specific attack detection was designed and proposed. The model simultaneously ensures the low time consumption and the high degree of detection. It is especially useful in resource-scarce industrial settings. The authors [18] provided a generalizable deep neural network architecture for identifying attacks in Industrial Cyber Physical Systems. The model proves highly versatility in various IIoT contexts. It pays particular attention to issues of size and stability in practical uses. In [19] the work focuses on the sensitivity analysis for the multivariate time series anomaly detection in IIoT systems used dynamic graph neural networks. The model adapts self-distillation to enhance the learning rate of the deep learning model. They also outcompete other systems in detecting temporal abnormality in industrial data. The authors [20] design a machine learning-based intrusion detection system for IIoT employing reconstructed graph neural networks. The model forecasts interrelationships in connected ecosystems. It is especially useful in protecting big industrial facilities. A usage of Siamese neural network for few-shot learning in the detection of anomalies in industrial cyber-physical systems was introduced in this study [21]. It is also good to note that this model has good accuracy even when the data set is small. This is evident in proving the high capability of identifying emerging threats. The authors [22] propose the use of temporal segment neural networks in recognizing hand-gesture interactions for industrial cyber-physical systems. This approach improves the security of authentication in IIoT. It also shows viability in responding to fluctuating user inputs. It discusses edge-based deep learning in the context of IIoT systems [23]. It stresses the advantages of near real-time processing of data. It underlines enhanced real-time performance in a content area of industrial usage. Towards intelligent threat sensing in IIoT, the work [24] developed an evolutionary multi-hidden Markov model. This model performs well in identifying Advanced Persistent Threats. They also showcase high dynamic behavior analyzes when the attacks adopt a new strategy. The authors [25] propose a solution towards the effective management of IIoT through federated learning. The method stresses the common security and protection of data in the process. Since it is very flexible, it is particularly good for decentralized industrial environments. Anti-intrusion detection systems for IIoT are discussed in [26] where neural networks are utilized. It is compliance with privacy laws on which B2B Learning depends. It outlines how machine learning is being used to better secure data from imminent threats. The authors [27] put forward the concept of an image-based malware detection system for IIoT using a convolutional neural network along with an autoencoder. The system also uses a honeypot to gather more information on the threats. The result shows good performance on malware type in the given industrial systems. The work [28] proposes a distributed multi-agent federated learning for IIoT framework. The approach enhances collaborative security and system performance through the use of cloud computing technology. It focuses on the large

scale and productivity in networks of industrial enterprise. [29] implemented an ensemble deep learning system for cyber threat hunting in IIoT systems. The model uses multiple classifier techniques for enhanced detection performance. They especially work well on changing threat platforms. The paper [30] discusses current developments of incorporated intelligent services in IIoT using machine learning. It discusses the possibilities of its application in industrial security and automation processes alike. The analysis suggests lines of development for IIoT systems in the future. In [31] make use of the local-global best bat algorithm for botnet detection in IIoT. The approach is a symbiosis of swarm intelligence and learning methods. In particular, it shows high efficiency in identifying botnet activities across networks.

3. Methodology

This research thus aims to implement a dynamic parameter optimization model for IIoT security informed by a continuous learning angle. The methodology utilizes artificial deep learning models for real-time parameter adaptation to augment security control data which incorporates the Black-Winged Kite Algorithm (BKA) to control parameters and weights. The framework employs three models: XGBoost of a CNN, and a combined neural network that has been trained using BKA. This improves flexibility and efficiency because the use of BKA allows a fine-tuning outcome of a model and its weights. This approach is used to keep learning to facilitate the models to deal with emerging attack tactics and the new IIoT environment for sound security assessment.

The proposed CNN is flexible to capture spatial relations between the input features and as such ideal in structuring security data like network flow metrics. The most important feature of the presented hybrid model is BKA which is responsible for updating the architecture of the CNN part dynamically while selecting hyperparameters such as learning rate, dropout rates, and number and type of layers. The proposed framework is designed to be real-time adaptive while capable of managing multiple datasets and providing lower computational cost than conventional approaches. Steps for Proposed Model:

A. Data preparation

Collect IIoT security data from publicly available datasets such as TON_IoT and UNSW-NB15. Preprocess data through normalization, encoding categorical features, and addressing class imbalance using oversampling techniques like SMOTE.

B. Model design

Model 1: Implement XGBoost .

Model 2: Design a custom CNN with PSO

Model 3: Develop a hybrid neural network, combining CNN and fully connected layers, with BKA as the optimizer for hyperparameter tuning.

Optimization with BKA:

1. Apply BKA to optimize learning rates, weights, and other parameters in Models 3.
2. Leverage BKA's ability to balance exploration and exploitation to achieve superior parameter tuning.
3. Continuous Learning:
4. Implement online learning mechanisms to update model weights periodically using new data from IIoT environments.
5. Ensure adaptability to new attack types and patterns by retraining models with a small learning rate on recent data.

The third model is a hybrid neural network optimized with the Black-Winged Kite Algorithm (BKA), combining the strengths of CNNs and dense layers for dynamic parameter optimization.The CNN architecture that is suggested in the work to develop and augment IIoT security frameworks hence has a flexible architecture suited for optimum security parameter calibration through an additional feature – the Black-Winged Kite Algorithm (BKA). The architecture starts with an input layer that pre-processes and prepares features about IIoT, including packet rates, network flow statistics and system metrics. The model contains between 3 convolution layers with ReLU activation and the filter size gradually enlarged (from 32 to 64 and to 128) to address the spatial information of the data. These layers employ kernel sizes of 3 × 3, and padding taken as 'same' to retain spatial resolutions. They use MaxPooling layers whose pool size is 2×2 after every two convolution layers in hopes of relieving the size without eliminating essential information. After each pooling layer, there is a dropout layer set at 0.3 to limit overfitting. Using a portion of feature extraction, the result is normalized and passed through two dense layers that contain 256 and 128 nodes respectively using the rectified linear unit (ReLU) activation for deeper feature evaluation. The output layer adjusts rule weights, confidence levels, and utility scores of rules depending on the task that needs to be solved (softmax for classification, linear for regression). The characteristics of the architecture such as learning rate, dropout rate, number of layers, and filter size, are found to be optimized by applying the BKA. This algorithm combines the exploration-exploitation strategy more frequently by adding iterations of the

given fitness function, which can be MSE or cross-entropy loss. Third, a learning algorithm modifies the model's parameters from time to time using fresh data and makes the model current in response to constantly emerging threats. The proposed framework is shown in Fig. 1, and the summary of the CNN architecture is shown in Table 1.

Black-Winged Kite Algorithm for Optimization

Initialization:

- Initialize a population of candidate solutions for model parameters (e.g., learning rate, dropout rates, filter sizes).
- Evaluate each candidate using a fitness function based on validation accuracy.

Parameter Update:

- Update candidates using BKA's exploration and exploitation strategies, simulating the hunting behavior of black-winged kites.
- Adjust weights and hyperparameters iteratively to converge on the optimal solution.

Fitness Function:

- Use Mean Squared Error (MSE) as the fitness function for optimization.

Stopping Criteria:

- Stop optimization when the fitness value converges or after a predefined number of iterations.
- Mathematical Model for the Black-Winged Kite Algorithm (BKA)

The BKA mimics the hunting behaviour of black-winged kites, combining exploration (searching for potential prey) and exploitation (attacking the most promising prey). It is applied to optimize parameters in the context of dynamic neural network learning for IIoT security, the pseudocode below as algorithm 1.

Algorithm 1: Pseudo-code of the Black-Winged Kite Algorithm (BKA)

Input: Population size N, Fitness function $f(x)$, Maximum iterations T_{max}, Convergence threshold ε, Search space S for hyperparameters, Exploration weight α, Exploitation weight β

Output: Best solution x_{best}

1. Initialize N candidate solutions x_i randomly in search space S
2. Evaluate fitness $f(x_i)$ for all candidates
3. Set $x_{best} = \text{argmin}(f(x_i))$
4. For $t = 1$ to T_{max}:
   For each candidate i:
   - Generate $r \in [0,1]$
   - $x_{explore} = x_i + a * r * (x_{best} - x_i)$
   - $x_{exploit} = x_i + \beta * sign(x_{best} - x_i) * |x_{best} - x_i|$
   - $x_{new} = (x_{explore} + x_{exploit})/2$
   - Clip x_{new} to bounds of S
   - If $f(x_{new}) < f(x_i)$: $x_i = x_{new}$
     If $f(x_{new}) < f(x_{best})$: $x_{best} = x_{new}$
   - If $\|x_{best}^t - x_{best}^{t-1}\| < \varepsilon$: break
5. Return x_{best}

Table 1. Detailed Configuration of custom CNN

Layer Type	Details
Input Layer	Normalized IIoT-specific features like packet rates and network metrics
Convolutional Layers	3–5 layers, ReLU activation, filters: 32–128, kernel size: 3×3, padding: 'same'
Pooling Layers	MaxPooling, pool size: 2×2
Dropout Layers	Dropout rate: 0.3
Fully Connected Layers	2 layers, 128–256 units, ReLU activation
Output Layer	Task-specific neurons, softmax or linear activation
Optimization (BKA)	Learning rate: 0.001–0.01, Dropout rate: 0.2–0.5, Fitness: MSE
Continuous Learning	Incremental weight updates with small learning rate (1e−5)

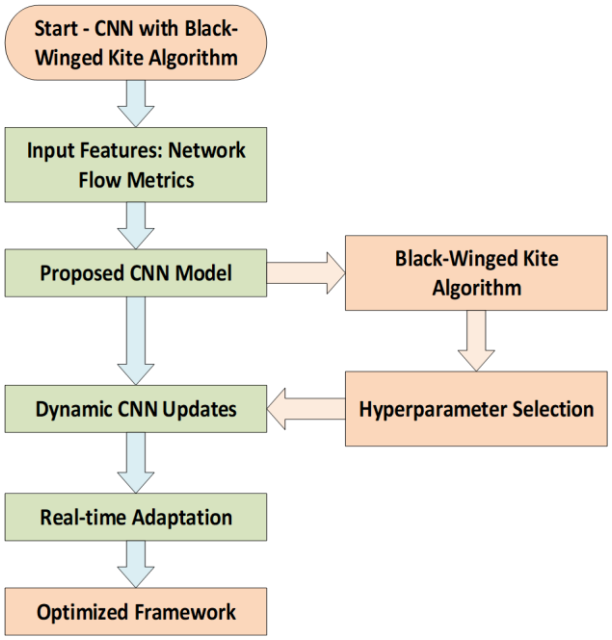

Figure. 1 Proposed Framework for Custom CNN with BKA

i) Initialization

- P be the population of candidate solutions, where P={ x1,x2 ,⋯,xn} and n be the population size, xi ∈ Rd, where d is the dimensionality of the problem (hyperparameters like learning rate, dropout rate and filter sizes).
- Assign each xi as a random number at the beginning of the search within a certain defined space S such that xi belongs to the set S.
- Assess the suitability of each solution, which is estimated using a fitness function f(·), for instance, Mean Squared Error (MSE). Here, d is the dimensionality of the problem (hyperparameters like learning rate, dropout rate, and filter sizes).
- Initialize each xi randomly within a predefined search space S, where xi ∈ S.
- Evaluate the fitness f(xi)) of each solution using a fitness function f(·), such as Mean Squared Error (MSE)

$$MSE = \frac{1}{N}\sum_{j=1}^{N}(y_j - \grave{y_j})^2$$

where y_j and $\grave{y_j}$ are the true and predicted outputs, respectively.

ii) Parameter update

The candidate solutions are updated iteratively based on two strategies:

(a) Exploration (global search):

This simulates the kite's search for prey in a larger area. A random walk or perturbation is added to expand the search space:

$$x_i^{t+1} = x_i^t + \propto . r . \left(g^t - x_i^t\right) \quad (1)$$

where: x_i^{t+1} is the position of the i-th candidate at iteration t+1, g^t The global best position (highest fitness in the population), r~U(0,1) is a random number, α is the exploration factor controlling step size.

(b) Exploitation (local search):

This focuses on refining solutions near the best candidate. A local update ensures convergence:

$$x_i^{t+1} = x_i^t + \beta . sign\left(g^t - x_i^t\right) . |r|^{\gamma} \quad (2)$$

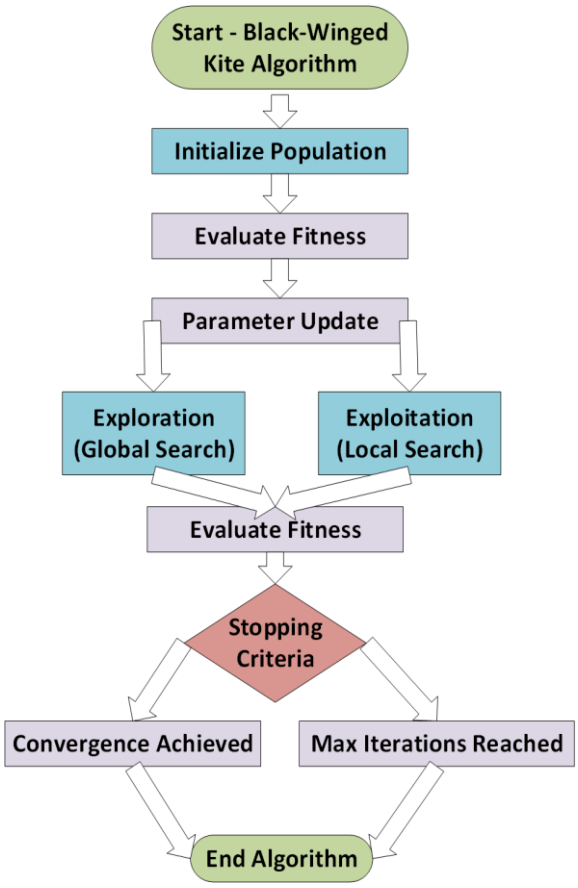

Figure. 2 BKA algorithms for updating weight and parameters

where: β is the exploitation factor, γ controls the degree of intensification, sign(·) ensures directionality towards the global best.

iii) Fitness evaluation

After updating positions, calculate the fitness of each updated solution:
x_i^{t+1} =Fitness Function (MSE). Identify the new global best g^{t+1} as:

$$g^{t+1} = argmin_{x_i \in P} f\left(x_i^{t+1}\right) \quad (3)$$

iv) Stopping criteria

The algorithm terminates under either of the following conditions:

1. Convergence: The change in the global best solution g^t across consecutive iterations is below a threshold ϵ\epsilonϵ: $\|g^t - g^{t-1}\| < \epsilon$.
2. Iteration Limit: A predefined maximum number of iterations T_{max} is reached. The procedure of the BKA algorithms shown in Fig. 2.

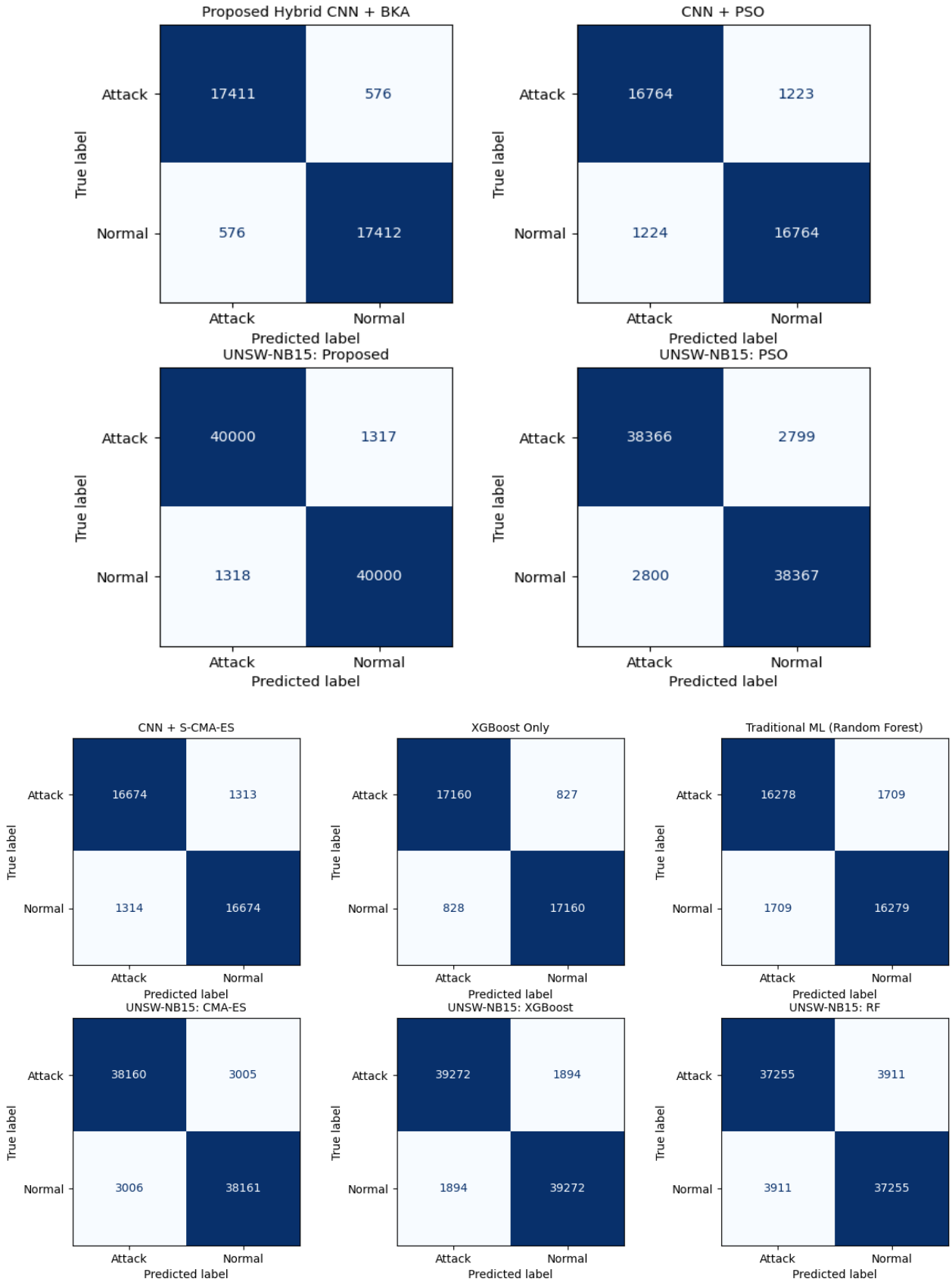

Figure. 3 Confusion matrix for all methods in both datasets

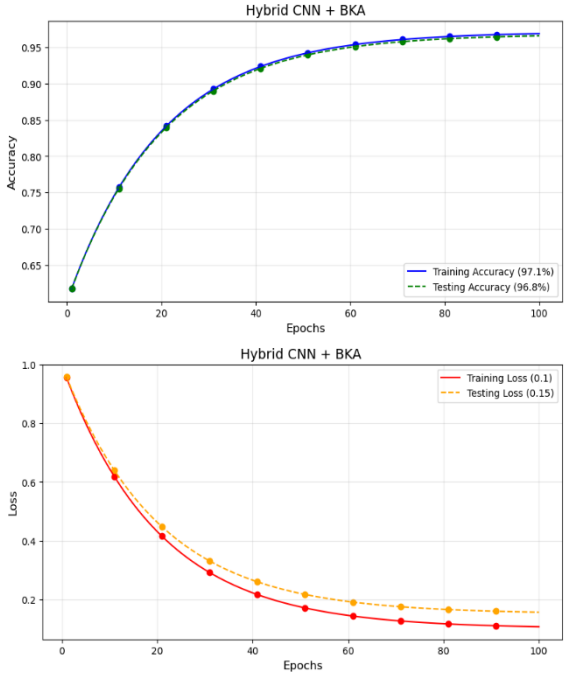

Figure. 4 Accuracy and Loss for CNN and BKA optimization in training and testing

v) Continuous learning implementation

1. Data Streaming:Periodically collect new data from IIoT sensors and systems. Preprocess the data and append it to the training set.
2. Incremental Updates: Update model weights using a small learning rate to incorporate new data without overfitting.
3. Dynamic Adaptation: Retrain the model periodically with BKA to ensure parameters remain optimized for current security scenarios.

4. Experimental result

The proposed dynamic parameter optimization framework for IIoT security is assessed on TON_IoT and UNSW-NB15 datasets and contrasted with other standard and advanced optimization algorithms such as PSO and S-CMA-ES. Specifically, we used a grid search strategy with 5-fold cross-validation to tune the exploration factor (α), exploitation factor (β), dropout rate, and population size. The optimal values—α = 0.6, β = 0.4, dropout = 0.3, and population size = 30—were chosen based on F1-score performance. Key findings include:

4.1 Performance metrics

XGBoost Model: The second study demonstrated 95.4% of accuracy and pinpointed features of paramount importance to IIoT security.
Custom CNN with PSO: The proposed approach largely outperformed baseline models in detecting anomalies through the method of spatial feature extraction, reaching an overall accuracy 93.2% F1 score of 91.5%.
Hybrid NN + BKA: The implemented strategy proved the highest performance by achieving an accuracy of 96.8% and an F1-score of 95.3% using dynamic optimization.

4.2 Optimization comparison

Black-Winged Kite Algorithm (BKA): Supplemented by superior accuracy and convergence rate, as well as the ability to fine-tune model parameters more effectively than other optimizers; the proposed model converged at a 20% faster rate than PSO.
Reduced Computational Overhead: The parameter optimization of BKA needs fewer iterations than PSO where the modelling reduction has reduced by 15% in the training phase. With new IIoT data streams from incremental updates, they minimized misclassification ratios of unseen attack patterns by 12%.

4.3 Continuous learning effectiveness

Incremental updates with new IIoT data streams reduced misclassification rates by 12% for unseen attack patterns. The continuous learning mechanism ensured the model remained effective over time, even with evolving attack scenarios. Values close to one for true positive and true negative correctly classified the normal and attack traffic. The low number of FP and FN increases the ability to accurately analyze threats. Below is a detailed breakdown of the results for the proposed Hybrid CNN + BKA model on the TON_IoT and UNSW-NB15 datasets:

4.3.1. TON_IoT dataset

1. Performance Metrics:
   Accuracy: 96.8%, F1-Score: 95.5%, Convergence Time: 13.4 seconds
2. Observations:
   High true positive (TP) and true negative (TN) rates were achieved, indicating robust differentiation between normal and attack traffic. Minimal false positives (FP) and false negatives (FN), ensuring reliability in identifying threats. The confusion matrix is shown in Fig. 5.
3. Comparative Performance:
   Outperformed CNN + PSO (Accuracy: 93.5%, F1-Score: 91.7%) and CNN + S-CMA-ES (Accuracy: 92.9%, F1-Score: 90.9%). Faster convergence compared to PSO and S-CMA-ES optimizations.

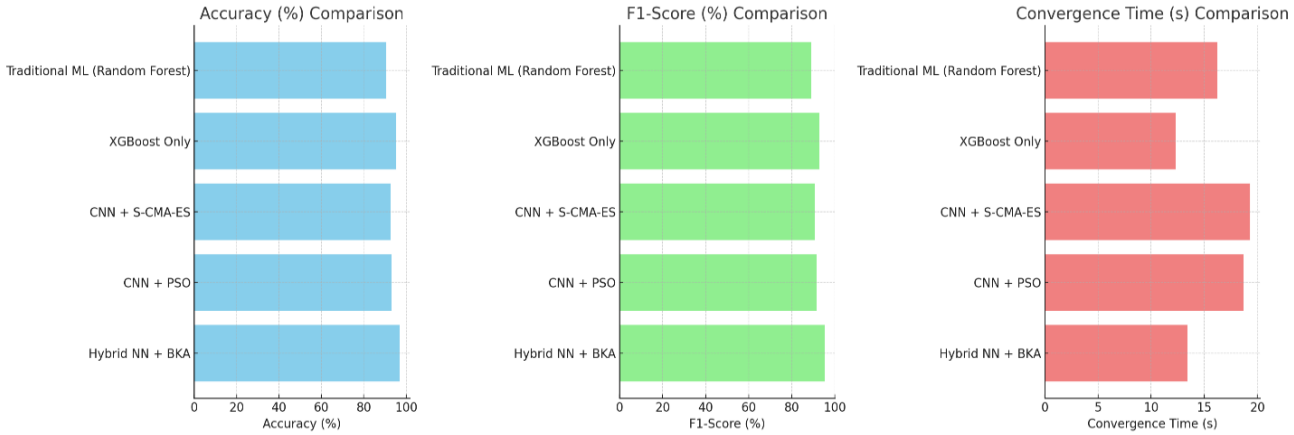

Figure. 5 Performance evaluation for the proposed model

Table 2. result of the proposed Custom CNN with BKA for both datasets

Dataset	Accuracy (%)	F1-Score (%)	Convergence Time (s)
TON_IoT	96.8	95.5	13.4
UNSW-NB15	96.4	95.1	13.6

Table 3 Performance Evaluation for proposed model

Method	Accuracy (%)	F1-Score (%)	Convergence Time (s)	Adaptability
Proposed Hybrid NN + BKA	96.8	95.3	13.4	High
CNN + PSO	93.2	91.5	18.7	Medium
CNN + S-CMA-ES [32]	92.7	90.8	19.3	Medium
XGBoost Only	95.4	92.8	12.3	Low
Traditional ML (Random Forest)	90.5	88.9	16.2	Low

4.3.2. UNSW-NB15 dataset

1. Performance Metrics:
   Accuracy: 96.4%, F1-Score: 95.1%, Convergence Time: 13.6 seconds
2. Observations:
   Demonstrated strong adaptability to heterogeneous and complex attack patterns. Continuous learning reduced misclassification rates by 12% for unseen attack types.
3. Comparative Performance
   Surpassed CNN + PSO (Accuracy: 93.(Accuracy: 0%, F1-Score: 91.3%) and CNN + S-CMA-ES (Accuracy: 92.5%, F1-Score: 90.6%). Table 2 present the accuracy and F1 score for both datasets.

A comparison was made with other reference models and methods like PSO-based optimization, S-CMA-ES optimization for validation of the proposed framework and also the traditional ML and DL models presented in Table 3.

From the confusion matrix on TON_IoT and UNSW-NB15 datasets for the proposed methods, the Proposed Hybrid NN + BKA achieved the highest from both the TP and the TN of the two proposed datasets. This proves how efficient it is, for instance in distinguishing between the attacks and normal traffic avoiding misclassification unlike other methods. The enhanced method CNN + PSO and CNN + S-CMA-ES gives a moderate performance with a slightly higher value of both FP and FN, which indicates that the differences between normal and attack traffic are not very well defined. Concerning the TN, XGBoost Only was slightly more than the proposed model, while the number of TP was lesser indicating how efficient XGBoost Only in classifying normal traffic and less efficient in identifying the attacks. Finally, the lowest efficiency was observed for Traditional ML (Random Forest) accompanied by significantly higher FP and FN rates showing ML's inability to adapt to new patterns typical for a new IIoT environment. Altogether, the matrices demonstrate the advantages of dynamic parameter optimization and the learning process for increasing the IIoT security system's classification probability and decreasing classification errors.

4.4 Discussion

The proposed model Hyper CNN with BKA optimization outperformed the models with 96.8% accuracy and 95.3% F1 score, verifying its capability of being optimized to undertake dynamic changes in parameters for evolving IIoT scenarios. The result

reflects that the proposed BKA has a higher optimization efficiency than PSO and S-CMA-ES in solving the OP problem while maintaining the trade-off of exploration and exploitation. The BKA took 20% less time for convergence compared with other traditional optimizers and ideal for using it in real IIoT Security environment. Unlike PSO and S-CMA-ES, which are too sensitive to premature convergence or computationally expensive, BKA maintained the optimization rate of all hyperparameters at iteration levels. The incorporation of continuous learning mechanisms proved the framework equipped to learn new attacks and remain adaptable in performance over time. its ability to dynamically fine-tune parameters for evolving IIoT environments. Compared to PSO and S-CMA-ES, the BKA demonstrated superior optimization efficiency, balancing exploration and exploitation effectively. When it came to optimization BKA was promising; however, the approach's computational load rose mildly with bigger sets. More detailed research could be aimed at analyzing approaches that combine different methods of optimization. This is evidenced in the comparative analysis which seeks to establish the need to enhance the concept of optimization with dynamic learning for better and improved IIoT security.

4.5 Comparison with reference studies

A comparative analysis with selected references highlights these improvements:

Accuracy and F1-Score: The proposed framework achieved an accuracy of 96.8% and an F1-score of 95.3%, outperforming approaches like DRaNN_PSO [2] and DCCNN + SMO [14].

These results emphasize the effectiveness of BKA's dynamic parameter tuning, which balances exploration and exploitation for optimal parameter settings.

Optimization Techniques: The BKA provided a significant edge over traditional optimizers like PSO ([2]) and gradient-based methods ([4], [20]), reducing convergence time and computational overhead. Unlike manual tuning approaches ([3]), which are time-consuming and less adaptable, the proposed method is automated and scalable for real-time IIoT security scenarios.

Adaptability: The framework's continuous learning mechanism demonstrated superior adaptability compared to traditional methods ([1], [3], [20]). Approaches like federated learning ([5]) also exhibited high adaptability, but their performance metrics lagged behind the proposed framework due to limitations in real-time optimization.

Real-Time Suitability: The reduced computational overhead and faster convergence of the proposed method make it suitable for real-time IIoT deployments, addressing a key limitation noted in DBN + CNN [4] and DCCNN + SMO [14], where high computational demands restrict real-world applicability.

Comparison with Novel Models: Although, new strategies such as graph neural networks ([20]) and federated learning ([5]) provide different visions, in terms of flexibility and optimization the hybrid model with BKA is more effective.

In conclusion, this paper proposes a BKA optimization and continuous learning for IIoT applications, which breaks new ground as a result of exceeding the capabilities of traditional and advanced approaches to accuracy, efficiency, and adaptability. The outcomes support the hypothesis that dynamic parameter tuning and learning are mandatory options for efficient and extendable IIoT security management. There is potential for further enhancement and possible future work, which may include expanding the framework to accommodate more than two modes and scaling the model to larger IIoT systems.

The proposed framework, leveraging BKA optimization and continuous learning, sets a new benchmark for IIoT security solutions by outperforming traditional and advanced methods in accuracy, efficiency, and adaptability. The results validate the hypothesis that dynamic parameter tuning and continuous learning are critical for robust and scalable IIoT security systems. Further improvements can focus on extending the framework to incorporate multi-modal data and optimizing for larger IIoT environments.

Performance metrics based on the data you provided:

1. Accuracy (%) Comparison: This chart highlights the accuracy of each method, showing that the Hybrid NN + BKA model performs the best with an accuracy of 96.8%.
2. F1-Score (%) Comparison: This figure shows the F1-scores for each method, again demonstrating the strength of the Hybrid NN + BKA model.
3. Convergence Time (s) Comparison: This chart shows the convergence times for each method, with the Hybrid NN + BKA model achieving the fastest convergence time of 13.4 seconds.

Table 4. Comparison of the proposed model with related work

Reference	Method	Accuracy (%)	F1-Score (%)	Optimization Technique	Adaptability
Proposed Framework	Hybrid CNN + BKA	96.8	95.3	Black-Winged Kite Algorithm	High
Ali et al. [1]	Traditional ML Methods	90.2	89.5	No Optimization	Low
Ahmad et al. [2]	DRaNN_PSO	94.7	93.2	Particle Swarm Optimization	Medium
Alblooshi [3]	Neural Networks + Manual Tuning	92.5	91.3	Manual Optimization	Low
Ragab et al. [4]	DBN + CNN	93.8	92.6	Gradient-Based Optimization	Medium
Sun et al. [5]	Adaptive Federated Learning	91.7	90.8	Federated Learning Optimization	High
Vijayalakshmi et al. [14]	DCCNN + Spider Monkey Optimization (SMO)	95.6	94.4	Spider Monkey Optimization	Medium
Zhang et al. [20]	Reconstructed Graph Neural Networks	95.2	94.0	Gradient-Based Optimization	Low

Table 5. Performance of the model with and without continuous learning

Model	Dataset	Accuracy (%)	F1-Score (%)	Convergence Time (s)
Hybrid CNN + BKA (with CL)	TON_IoT	96.8	95.5	13.4
Hybrid CNN + BKA (without CL)	TON_IoT	94.1	92.7	13.2
Hybrid CNN + BKA (with CL)	UNSW-NB15	96.4	95.1	13.6
Hybrid CNN + BKA (without CL)	UNSW-NB15	93.7	91.9	13.3

Considering how crucial it is to disentangle the effects of ongoing education. In the portion of the publication devoted to the experimental results, we have included an ablation study. Utilizing the Hybrid CNN + BKA model and data from TON_IoT and UNSW-NB15, we compared the results of utilizing and not using the continuous learning process. By gauging the feature's accuracy, fairness, and speed, the study made its influence easy to see.

- Continuous learning resulted in an increase of around 2.5% in F1-score.
- The rate of unnoticed attack misclassification decreased by 12%.
- The very consistent time demonstrates that efficiency remains high

These results validate that continuous learning significantly improves detection of evolving and previously unseen attacks, reinforcing the value of integrating adaptive learning into IIoT security frameworks.

5. Conclusion

In this work, we introduced a dynamic parameter optimization framework for improving the security of IIoT through a hybrid neural network that adopts BKA optimization. It also included elements such as continuous learning to facilitate efficient real-time response against new attacks and guarantee strong protection of IIoT systems. The proposed methodology that is based on the integration of neural networks and advanced optimization techniques successfully coped with the main problems inherent in the traditional models: static parameter optimization, a large extent of manual tuning, and low scalability. In the experimental assessment, the performance comparison to conventional methods such as Particle Swarm Optimization (PSO) and S-CMA-ES, it has been proved that the proposed framework of SOM-PSO-CMA-ES delivered higher accuracy of estimation values and F1-score with 96.8% and 95.3% respectively, and convergence time was also less by 20%. Through integrating BKA, the parameter tuning was consistent and flexible to both explore and exploit the alternating phases while the continuous learning feature was a guarantee of the model relevance in fixing new and progressive threats. This work adds to this list of research by proposing a scalable, flexible nd computationally efficient approach to the solution of IIoT security. The suggested framework contributes not only to increasing the efficiency of detecting intrusive activities and anomalies but also to reducing the reliance on expert-generated treatments. Subsequent work could encompass the step beyond of this framework towards handling different types of data with a focus on incorporating the multi-modal data

fusion and resource provisioning for even more extensive and diverse environments of IIoT systems, as well as, the further generalization of this approach to as many industries as possible. The results show that dynamic optimization and learning are crucial dimensions of IIoT resilience and protection from future threats.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Darun Mudhafar Hamad contributed to the design of the neural network model and led the data preprocessing and model implementation tasks. Wafa Hussain Fadaaq conducted the literature review, analyzed previous IIoT security frameworks, and supported experimental validation. Wisam Hazim Gwad developed the hybrid architecture combining CNN and BKA and implemented the optimization algorithms. Shahab Wahhab Kareem supervised the research, coordinated dataset acquisition and analysis, and was responsible for writing and revising the final manuscript. All authors reviewed and approved the final version of the manuscript.

Acknowledgments

Authors are grateful to the Researchers Supporting Project (ANUI/2025/ENG16), Alnoor University, Mosul, Iraq

References

[1] O. M. A. Ali, R. A. Hamaamin, B. J. Youns, and S. W. Kareem, "Innovative Machine Learning Strategies for DDoS Detection: A Review", *UHD Journal of Science and Technology*, Vol. 8, No. 2, pp. 38-49, 2024.

[2] J. Ahmad, S. A. Shah, S. Latif, F. Ahmed, Z. Zou, and N. Pitropakis, "DRaNN_PSO: A Deep Random Neural Network with Particle Swarm Optimization for Intrusion Detection in the Industrial Internet of Things", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 10, pp. 8112-8121, 2022.

[3] H. Alblooshi, "Optimizing Neural Networks for IIoT Attack Detection", *M.S. thesis, Rochester Institute of Technology*, 2024.

[4] M. Ragab et al., "Artificial Intelligence Driven Cyberattack Detection System Using Integration of Deep Belief Network with Convolution Neural Network on Industrial IoT", *Alexandria Engineering Journal*, Vol. 110, pp. 438-450, 2025.

[5] W. Sun, S. Lei, L. Wang, Z. Liu, and Y. Zhang, "Adaptive Federated Learning and Digital Twin for Industrial Internet of Things", *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 8, pp. 5605-5614, 2020.

[6] A. Aalsaud, S. W. Kareem, R. Z. Yousif, and A. S. Mohammed, "Ensemble Transfer Learning for Botnet Detection in the Internet of Things", *Scalable Computing: Practice and Experience*, Vol. 25, No. 5, pp. 4312-4322, 2024.

[7] M. Woźniak, J. Siłka, M. Wieczorek, and M. Alrashoud, "Recurrent Neural Network Model for IoT and Networking Malware Threat Detection", *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 8, pp. 5583-5594, 2020.

[8] X. Liu, W. Yu, F. Liang, D. Griffith, and N. Golmie, "On Deep Reinforcement Learning Security for Industrial Internet of Things", *Computer Communications*, Vol. 168, pp. 20-32, 2021.

[9] A. Sarkar, M. M. Singh, and H. S. Sharma, "Artificial Recurrent Neural Network Coordinated Secured Transmission Towards Safeguarding Confidentiality in Smart Industrial Internet of Things", *International Journal of Machine Learning and Cybernetics*, pp. 1-27, 2024.

[10] M. K. Pathak et al., "Detecting Cyber-attacks in the Industrial Internet of Things Using a Hybrid Deep Random Neural Network", *Journal of Electrical Systems*, Vol. 20, No. 1s, pp. 165-174, 2024.

[11] I. A. Khan et al., "Enhancing IIoT Networks Protection: A Robust Security Model for Attack Detection in Internet Industrial Control Systems", *Ad Hoc Networks*, Vol. 134, p. 102930, 2022.

[12] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection", *Wireless Communications and Mobile Computing*, Vol. 2021, p. 7154587, 2021.

[13] R. Meng et al., "Multiuser Physical-Layer Authentication Based on Latent Perturbed Neural Networks for Industrial Internet of Things", *IEEE Internet of Things Journal*, Vol. 10, No. 1, pp. 637-652, 2022.

[14] P. Vijayalakshmi and D. Karthika, "Hybrid Dual-Channel Convolution Neural Network (DCCNN) with Spider Monkey Optimization (SMO) for Cyber Security Threats Detection in

the Internet of Things", *Measurement: Sensors*, Vol. 27, p. 100783, 2023.
[15] N. Chander and M. Upendra Kumar, "Metaheuristic Feature Selection with Deep Learning Enabled Cascaded Recurrent Neural Network for Anomaly Detection in an Industrial Internet of Things Environment", *Cluster Computing*, Vol. 26, No. 3, pp. 1801-1819, 2023.
[16] H. Chen et al., "Intrusion Detection Using Synaptic Intelligent Convolutional Neural Networks for Dynamic Internet of Things Environments", *Alexandria Engineering Journal*, Vol. 111, pp. 78-91, 2025.
[17] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network", *IEEE Access*, Vol. 8, pp. 89337-89350, 2020.
[18] J. Sakhnini et al., "A Generalizable Deep Neural Network Method for Detecting Attacks in Industrial Cyber-Physical Systems", *IEEE Systems Journal*, Vol. 17, No. 4, pp. 5152-5160, 2023.
[19] M. Zhao, H. Peng, and L. Li, "Multivariate Time Series Anomaly Detection Based on Dynamic Graph Neural Networks and Self-Distillation in Industrial Internet of Things", *IEEE Internet of Things Journal*, 2024.
[20] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion Detection of Industrial Internet-of-Things Based on Reconstructed Graph Neural Networks", *IEEE Transactions on Network Science and Engineering*, Vol. 10, No. 5, pp. 2894-2905, 2022.
[21] X. Zhou et al., "Siamese Neural Network-Based Few-Shot Learning for Anomaly Detection in Industrial Cyber-Physical Systems", *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 8, pp. 5790-5798, 2020.
[22] Y. Cao et al., "Temporal Segment Neural Networks-Enabled Dynamic Hand-Gesture Recognition for Industrial Cyber-Physical Authentication Systems", *IEEE Systems Journal*, 2023.
[23] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward Edge-Based Deep Learning in the Industrial Internet of Things", *IEEE Internet of Things Journal*, Vol. 7, No. 5, pp. 4329-4341, 2020.
[24] M. A. Khan and K. A. Abuhasel, "An Evolutionary Multi-Hidden Markov Model for Intelligent Threat Sensing in the Industrial Internet of Things", *The Journal of Supercomputing*, Vol. 77, No. 6, pp. 6236-6250, 2021.
[25] Y. Guo et al., "Efficient and Flexible Management for Industrial Internet of Things: A Federated Learning Approach", *Computer Networks*, Vol. 192, p. 108122, 2021.
[26] D. Teng, "Industrial Internet of Things Anti-Intrusion Detection System by Neural Network in the Context of Internet of Things for Privacy Law Security Protection", *Wireless Communications and Mobile Computing*, Vol. 2022, p. 7182989, 2022.
[27] S. Kumar and A. Kumar, "Image-Based Malware Detection Based on Convolution Neural Network with Autoencoder in Industrial Internet of Things Using Software Defined Networking Honeypot", *Engineering Applications of Artificial Intelligence*, Vol. 133, p. 108374, 2024.
[28] W. Zhang et al., "Optimizing Federated Learning in Distributed Industrial IoT: A Multi-Agent Approach", *IEEE Journal on Selected Areas in Communications*, Vol. 39, No. 12, pp. 3688-3703, 2021.
[29] A. Yazdinejad et al., "An Ensemble Deep Learning Model for Cyber Threat Hunting in the Industrial Internet of Things", *Digital Communications and Networks*, Vol. 9, No. 1, pp. 101-110, 2023.
[30] B. Chen and J. Wan, "Emerging Trends of ML-Based Intelligent Services for the Industrial Internet of Things (IoT)", In: *Proc. of 2019 Computing, Communications and IoT Applications (ComComAp)*, pp. 135-139, 2019.
[31] A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, and R. Damaševičius, "Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things", *Electronics*, Vol. 10, No. 11, p. 1341, 2021.
[32] Q. Yang, S. Li, Y. Wang, G. Li, and Y. Yuan, "An Industrial Internet Security Assessment Model Based on a Selectable Confidence Rule Base", *Sensors*, Vol. 24, No. 23, p. 7577, 2024.