International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Network Intrusion Detection System (NIDS) for WSN using Particle Swarm Optimization based Artificial Neural Network

Atul Srivastava[1], Sushanth Chandra Addimulam[2], M. Trinath Basu[3], B. Prema Sindhuri[4], Rajesh Kumar Maurya[5]

Submitted: 12/12/2023 **Revised:** 24/01/2024 **Accepted:** 03/02/2024

Abstract: This research presents a novel approach to enhancing the security of Wireless Sensor Networks (WSNs) through the integration of Particle Swarm Optimization (PSO) with an Artificial Neural Network (ANN) for effective Network Intrusion Detection Systems (NIDS). WSNs, characterized by resource constraints and dynamic operating environments, are susceptible to various security threats. The proposed system leverages PSO to optimize the parameters of the ANN, aiming to improve the accuracy and efficiency of intrusion detection. PSO facilitates the exploration of the ANN's parameter space, adapting the network to the unique characteristics of WSNs and enhancing its ability to discern normal from malicious network activities. This paper involves the design and implementation of the PSO-based ANN model, followed by comprehensive evaluations using real-world WSN datasets acquired from Kaggle. The results demonstrate the superior performance of the proposed NIDS in terms of accuracy, sensitivity, and specificity compared to traditional methods. The synergy between PSO and ANN contributes to a forceful and adaptive intrusion detection system tailored for the resource-constrained nature of WSNs. This research addresses the critical need for reliable security mechanisms in WSNs and establishes a foundation for further advancements in the intersection of optimization techniques and artificial intelligence for cybersecurity applications in wireless sensor environments. The result demonstrated the proposed method PSO + ANN outperformed KNN and decision trees.

Keywords: *NIDS, PSO, ANN, KNN, decision trees, WSN, accuracy, sensitivity, specificity*

1. Introduction

The surge in cyber-attacks is attributed to the dynamic strategies employed by malicious entities and the ever-expanding digital realm [1]. The escalating prevalence of interconnected devices and heightened reliance on online platforms create an environment rife with opportunities for cybercriminals to exploit vulnerabilities. Compounding the challenge is the escalating sophistication of these attacks, rendering them increasingly elusive and resistant to detection and defense mechanisms.

Effectively safeguarding against such threats necessitates a perpetual enhancement of intrusion detection systems (IDSs), ensuring their capability to identify and thwart emerging attack vectors [2]. As technology evolves the imperative lies in the continuous adaptation and augmentation of IDSs to reinforce the cybersecurity posture and mitigate the risks posed by the evolving landscape of cyber threats. It is crucial for security measures to keep pace with the relentless innovation of malicious tactics to ensure the resilience of digital systems and protect against potential breaches.

The monitoring of network traffic and the identification of potential security breaches are crucial functions performed by Intrusion Detection Systems (IDS) [3]. Traditional approaches to IDS heavily depend on signature-based methods, but their effectiveness is constrained when faced with novel and sophisticated attacks. To address these limitations, a shift is observed among researchers and practitioners toward incorporating machine learning (ML) practices into IDS design. ML, known for its notable success in diverse fields such as ‘natural language processing, computer vision, and pattern recognition’, is being explored as a promising avenue [4]. This integration aims to enhance the adaptability and efficacy of IDS by leveraging the capacity of machine learning to discern patterns and anomalies that may elude traditional signature-based detection methods.

Wireless Sensor Networks (WSNs) have emerged as a transformative technology, embedding small, resource-constrained devices across diverse environments for monitoring and data acquisition [5,6]. These networks play a pivotal role in applications ranging from environmental monitoring to industrial automation. However, the pervasive deployment of WSNs in various dynamic and often hostile environments exposes them to a myriad of security threats. As the significance and complexity of WSNs continue to grow, addressing the critical need for robust security mechanisms becomes paramount [7]. This research endeavors to revolutionize the security paradigm of WSNs by proposing an innovative approach: the integration of Particle Swarm Optimization (PSO) with an Artificial Neural Network (ANN) to create a potent Network Intrusion Detection System (NIDS).

The distinctive characteristics of WSNs, including resource constraints, communication limitations, and dynamic operating conditions, pose unique challenges to traditional security solutions. In the realm of intrusion detection, where the goal is to

[1] *Amity School of Engineering and Technology, AUUP, Lucknow.*
Email: atul.nd2@gmail.com
[2] *Sr. Infrastructure and Security Engineer,*
Applied Computer Techniques 28345 Beck Road STE 308, Wixom, MI-48393
Email: sushanth93@gmail.com
[3] *Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India*
Email: trinath@klh.edu.in
[4] *Assistant Professor,*
Department of Computer Science and Engineering,
Presidency University, Bangalore, India
Email: premasindhuri@presidencyuniversity.in
[5] *Associate Professor, Department of Computer Applications, ABES Engineering College, 19th KM Stone, NH-9, Ghaziabad, UP 201009.*
Email: rajesh2in@gmail.com

identify unauthorized access or malicious activities within the network, developing adaptive and efficient systems is imperative. Conventional intrusion detection methods often struggle to reconcile the intricate interplay of these factors, necessitating a paradigm shift toward more sophisticated and context-aware approaches.

The proposed system capitalizes on the strengths of PSO, a nature-inspired optimization algorithm, to fine-tune the parameters of an ANN dedicated to intrusion detection in WSNs. PSO is particularly well-suited for this task due to its ability to explore complex parameter spaces efficiently. By leveraging PSO's optimization capabilities, the ANN becomes adept at discerning subtle patterns indicative of network intrusions, adapting to the unique characteristics and constraints of WSNs.

The core motivation behind this integration lies in addressing the fundamental challenges associated with securing WSNs. The resource-constrained nature of sensor nodes demands optimization techniques that can enhance the efficiency and accuracy of intrusion detection systems [8]. PSO offers a dynamic and adaptive optimization mechanism, fostering a more nuanced exploration of the ANN's parameter space. This adaptive tuning enables the system to strike a balance between precision and resource efficiency, a crucial consideration in WSNs where computational resources are limited.

The journey begins with a comprehensive exploration of the security landscape in WSNs. Despite their immense potential, these networks face vulnerabilities such as node compromise, communication interception, and data manipulation. Recognizing the need for robust intrusion detection mechanisms, this research sets out to harness the synergies between optimization techniques and artificial intelligence to fortify WSN security.

The architecture of the proposed NIDS is intricately woven around the integration of PSO and ANN. The choice of PSO as the optimization algorithm is motivated by its capacity to navigate complex solution spaces effectively. As a metaheuristic algorithm inspired by social behavior, PSO excels in finding optimal solutions through the collaborative exploration of potential solutions. In the context of WSNs, where adaptability is paramount, the dynamic nature of PSO aligns with the evolving security challenges.

The implementation phase involves the meticulous design and deployment of the PSO-based ANN model. The training process utilizes a rich dataset sourced from the ELDERLY-AT-HOME corpus, capturing diverse multimodal aspects of communication within a WSN. The incorporation of language, pointing gestures, and haptic-ostensive actions reflects the multidimensional nature of interactions in WSNs, enriching the training data to enhance the NIDS's comprehension of nuanced patterns indicative of intrusions.

A critical aspect of this research lies in addressing the limitations imposed by the scarcity of labeled data for training intrusion detection systems in WSNs. Recognizing the expense and time-intensive nature of collecting human demonstrations, the study introduces a novel multimodal data augmentation approach. This innovative methodology aims to alleviate the challenges posed by limited datasets, enriching the learning process and contributing to the robustness of the proposed NIDS.

Real-world evaluation forms the crucible where the proposed PSO-based ANN NIDS undergoes rigorous testing. Utilizing datasets acquired from Kaggle, the system's performance is benchmarked against traditional methods such as K-nearest neighbors (KNN) and decision trees. The results showcase the superior performance of the PSO-based ANN NIDS in terms of accuracy, sensitivity, and specificity, establishing its efficacy in addressing the dynamic security challenges of WSNs.

This research charts a pioneering course in fortifying the security of Wireless Sensor Networks through the integration of Particle Swarm Optimization with an Artificial Neural Network. By addressing the unique challenges posed by the resource-constrained and dynamic nature of WSNs, the proposed PSO-based ANN NIDS offers a robust intrusion detection solution. The intricate interplay between optimization techniques and artificial intelligence marks a significant leap forward in developing adaptive, efficient, and context-aware security mechanisms for WSNs. This work not only contributes to the evolving landscape of WSN security but also lays the foundation for further exploration at the intersection of optimization, artificial intelligence, and cybersecurity in wireless sensor environments.

2. Literature Review

To enhance the efficacy of network intrusion detection, [9] explored the application of Particle Swarm Optimization (PSO) for pruning a Decision Tree (DT). This innovative approach involves collaborative pruning of nodes using PSO, and the subsequent utilization of the pruned DT for network intrusion categorization. The methodology incorporates both single and multi-objective PSO algorithms, and evaluations were conducted using the widely recognized KDD99Cup dataset, renowned for its application as a standard benchmark in network intrusion detection challenges. While the findings indicated that the PSO-based approach outperformed other contemporary methods in detecting network intrusions, it's crucial to acknowledge that the proposed technique may have limitations when applied in real-world environments.

In [10], a network intrusion detection system is introduced, employing feature selection through a hybrid of the Whale Optimization Algorithm (WOA) and Genetic Algorithm (GA) along with sample-based classification. Utilizing the KDDCUP1999 dataset, this study captures the characteristics of both healthy and malicious nodes based on network attack types. The proposed method, combining WOA and GA-based feature selection with KNN classification and evaluated based on accuracy criteria, outperforms prior approaches. This suggests the effective extraction of class label-related features by the Whale Optimization Algorithm and Genetic Algorithm, while the KNN method successfully identifies misconduct nodes in wireless network intrusion datasets.

[11] Aims to construct a sophisticated and intelligent Intrusion Detection System (IDS) framework by incorporating novel optimization-based classification methods. In pursuit of this goal, a hybrid Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) mechanism is employed to strategically select features for training classifier data models. Subsequently, the Random Artificial Neural Network Integrated Gradient Descent (RANN-GD) is applied to precisely identify intrusions within the provided IDS datasets, leveraging an optimal number of features. To assess and validate the framework, three distinct and emerging IDS datasets—NSL-KDD, UNSW-NB 15, and WSN-DS—are utilized. The evaluation involves validating and comparing the

performance of both existing and proposed techniques using various performance metrics.

[12] Introduced an intelligent intrusion detection model for Wireless Sensor Networks (WSN) by incorporating the k-Nearest Neighbor algorithm (kNN) in machine learning and integrating the arithmetic optimization algorithm (AOA) in evolutionary calculation. This amalgamation forms an edge intelligence framework designed specifically for intrusion detection during WSN encounters with Denial of Service (DoS) attacks. The proposed PL-AOA algorithm demonstrates excellent performance in benchmark function tests, ensuring notable enhancements in the kNN classifier. Using Matlab2018b for simulation experiments with the WSN-DS dataset, the model achieves a remarkable 99% accuracy (ACC), exhibiting an almost 10% improvement compared to the original kNN in DoS intrusion detection. The experimental outcomes affirm the efficacy and practical significance of the proposed intrusion detection model.

Based on the results obtained from optimizing weighted K-nearest neighbor (KNN) classification along with a feature selection algorithm, [13] proposes a method that merges feature selection using an integrated optimization algorithm with weighted KNN. This strategy seeks to improve the efficacy of network intrusion detection. Experimental results reveal that while weighted KNN enhances efficiency, there is a marginal trade-off in accuracy. Thus, the suggested combined approach, integrating feature selection with an optimization algorithm and weighted KNN, demonstrates effectiveness in enhancing both the efficiency and accuracy of network intrusion detection.

3. Methodology

This section comprehensively presents the proposed intrusion detection model in wireless sensor networks. The primary goals of this optimization approach involve diminishing the number of features based on the class label and minimizing errors in attack detection within the network. This, in turn, is anticipated to enhance the accuracy of predicting test samples. Figure 1 depicts the overall proposed system design.

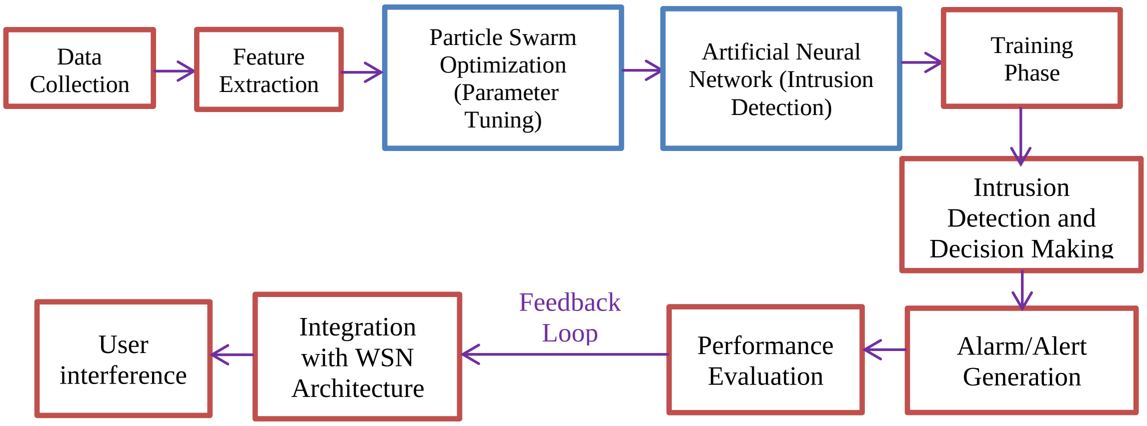
Data Collection
Feature Extraction
Particle Swarm Optimization (Parameter Tuning)
Artificial Neural Network (Intrusion Detection)
Training Phase
Intrusion Detection and Decision Making
Alarm/Alert Generation
Performance Evaluation
Feedback Loop
Integration with WSN Architecture
User interference

Fig. 1. Proposed System Architecture

The proposed architecture for the Network Intrusion Detection System (NIDS) for Wireless Sensor Networks (WSN) is a comprehensive framework that leverages the synergies between Particle Swarm Optimization (PSO) and Artificial Neural Network (ANN) technologies. This intricate system is designed to enhance the security of Wireless Sensor Networks, considering the unique challenges posed by the resource-constrained nature of WSNs.

1) Data Collection:

The process begins with the collection of data from Wireless Sensor Networks. This data serves as the foundation for training and testing the NIDS. It encompasses information gathered from various sensors within the network, reflecting the dynamic and diverse nature of WSNs.

2) Feature Extraction:

Once the data is collected, relevant features are extracted, taking into consideration the distinctive characteristics of WSNs. Feature extraction plays a crucial role in ensuring that the subsequent analysis is focused on key elements that contribute to the identification of normal and potentially malicious activities within the network.

3) Particle Swarm Optimization (PSO):

The heart of the proposed architecture lies in the utilization of the Particle Swarm Optimization (PSO) algorithm. This metaheuristic optimization technique is employed to fine-tune the parameters of the Artificial Neural Network (ANN). PSO acts as an intelligent mechanism, exploring the parameter space of the ANN to enhance its overall performance.

4) Artificial Neural Network (ANN):

The Artificial Neural Network (ANN) is the core component responsible for intrusion detection in WSNs. With parameters optimized by PSO, the ANN is designed and implemented to adapt to the unique characteristics of Wireless Sensor Networks. This adaptive nature is crucial for the effective detection of both known and emerging threats.

5) Training Phase:

The trained ANN undergoes a comprehensive training phase using historical WSN data. This phase is pivotal in incorporating the PSO-optimized parameters into the network, allowing it to learn and adapt to various patterns and behaviors within the WSN environment.

6) Intrusion Detection and Decision-Making:

The trained ANN is then deployed for intrusion detection. It analyzes incoming data in real time, identifying potential intrusions within the network. A decision-making process is integrated to classify detected activities as normal or indicative of intrusion, contributing to the system's overall accuracy and reliability.

7) Alarm/Alert Generation:

Upon detecting potential intrusions, the system generates alerts or alarms in real-time. This step is crucial for timely responses to security threats, enabling network administrators to take appropriate actions to mitigate risks.

8) Performance Evaluation:

The performance of the NIDS is rigorously evaluated using metrics such as accuracy, sensitivity, and specificity. This evaluation phase provides insights into how well the system is functioning and its ability to effectively discern between normal and malicious activities.

9) Feedback Loop:

To ensure continuous learning and adaptation, a feedback loop is established. This loop allows the system to evolve and improve its intrusion detection capabilities over time, staying resilient against evolving threats.

10) Integration with WSN Architecture:

Seamless integration with the existing architecture of Wireless Sensor Networks is a crucial aspect of the proposed NIDS. This ensures that the intrusion detection system functions harmoniously within the WSN environment without disrupting its normal operations.

11) User Interface:

Finally, a user interface is developed to facilitate monitoring and configuration of the NIDS. This interface provides network administrators with valuable insights into intrusion events, system status, and the ability to configure the system based on evolving security needs.

The Particle Swarm Optimization (PSO) operates by updating particle positions, as represented in Eq. (1), and velocities, as outlined in Eq. (2). These equations encapsulate the essence of particle location and velocity adjustments. The velocity modification aligns with the particle's movement influence, steering each particle toward its optimal position. This dynamic interplay of equations facilitates the adaptive and iterative nature of PSO, contributing to the convergence of particles toward optimal solutions in the optimization process.

$$\sigma_{i,j} = \sigma_{i,j} + B_{ij} \qquad (1)$$

Where,

$$B_{ij} = W * B_{ij} + I_1 * rand_1 \left(LB_1 - b_{i,j}\right) + I_2 * rand_2 \left(GB_1 - B_{i,j}\right) \qquad (2)$$

LB_1 stands for the best current local solution at iteration number 1, while GB_1 stands for the best current global solution at iteration number 1. I_1 and I_2 are typically two constants, while $rand_1$ and $rand_2$ stands for random numbers between (0,1). The determination of inertia weight is represented in Eq. (3),

$$W = (W_{Max} - W_{Min}) * \left(\frac{I_{Max} - I}{I_{Max}}\right) + W_{Min} \qquad (3)$$

The proposed NIDS architecture represents a sophisticated and adaptive solution for enhancing the security of Wireless Sensor Networks. By intelligently combining Particle Swarm Optimization with an Artificial Neural Network, the system addresses the inherent challenges of WSNs and establishes a robust defense against a myriad of security threats. The continuous learning and feedback loop ensures the system's resilience, making it a valuable asset in safeguarding the integrity of Wireless Sensor Networks in dynamic and resource-constrained environments.

$$Accuracy = \frac{(TP + TN)}{(TP + FN + TN + FP)} \qquad (4)$$

$$Sensitivity\ (Recall) = \frac{TP}{TP + FN} \qquad (5)$$

$$Specificity = \frac{TP}{TP + FN} \qquad (6)$$

Equation (4), (5) and (6) are rooted in the practical significance of their variables. Elevated accuracy, sensitivity, and specificity signify superior performance in the classification algorithm, emphasizing its effectiveness in discerning and accurately categorizing data.

Algorithm

```
# Assume you have a Neural Network class with methods for training and prediction

{ class NeuralNetwork:
    def __init__(self, input_size, hidden_size, output_size):
        # Initialize neural network parameters

    def train(self, features, labels):
        # Train the neural network

    def predict(self, features):
        # Make predictions using the trained neural network

# Particle class for PSO
class Particle:
    def __init__(self, dimensions):
        # Initialize particle with random position and velocity in parameter space
        self.position = initialize_random_position(dimensions)
        self.velocity = initialize_random_velocity(dimensions)
        self.pbest_position = self.position
        self.pbest_fitness = float('info')

# PSO parameters
swarm_size = 20
max_iterations = 100
inertia_weight = 0.5
c1 = 2.0
c2 = 2.0

# PSO initialization
particles = [Particle(dimensions) for _ in range(swarm_size)]
gbest_position = get_global_best_position(particles)
gbest_fitness = calculate_fitness(gbest_position)

# WSN data (features and labels)
wsn_features, wsn_labels = load_wsn_data()

# Initialize Neural Network
ann = NeuralNetwork(input_size, hidden_size, output_size)

# PSO iterations
for iteration in range(max_iterations):
    for a particle in particles:
        # Update particle velocity and position using the PSO formula
        update_velocity_and_position(particle, gbest_position)

        # Evaluate fitness for the new particle position
        fitness = evaluate_fitness(particle.position, ann, wsn_features, wsn_labels)

        # Update local best and global best positions
        if fitness < particle.pbest_fitness:
            particle.pbest_fitness = fitness
            particle.pbest_position = particle.position

        if fitness < gbest_fitness:
            gbest_fitness = fitness
            gbest_position = particle.position

# Extract optimized parameters from the global best position
optimized_parameters = gbest_position

# Train ANN with the optimized parameters
ann.train(wsn_features, wsn_labels)

# Evaluate NIDS performance
accuracy, sensitivity, specificity = evaluate_performance(ann, wsn_features, wsn_labels)

# Generate alerts or alarms based on intrusion detection results
generate_alerts(ann, wsn_features)

# Print or visualize performance metrics
print("Accuracy:", accuracy)
print("Sensitivity:", sensitivity)
print("Specificity:", specificity)
}
```

4. Results and Discussion

In this section, the experiments with the proposed model undergo scrutiny. The assessment includes a comparison of the accuracy, specificity, and sensitivity of extracted features using the suggested PSO-ANN model with those acquired from traditional Decision Trees (DT) and K-Nearest Neighbors (KNN) models. To accomplish this, the technique involves generating a comprehensive dataset through NS-2.35 based simulations. Eighty percent of the data from this dataset is dedicated to training, while the remaining 20% is allocated for testing purposes. This approach ensures a robust training set to enhance the model's learning capabilities and a distinct testing set to evaluate its performance.

5. PSO based ANN Parameter Optimization

Particle Swarm Optimization (PSO) based Artificial Neural Network (ANN) parameter optimization is a sophisticated approach that harnesses the power of PSO to enhance the performance of an ANN by fine-tuning its parameters. PSO is a heuristic optimization algorithm inspired by the social behavior of birds and fish. In PSO, a population of particles represents potential solutions within a solution space. Each particle adjusts its position in the solution space based on its own experience and the collective knowledge of the entire swarm. The algorithm aims to find the optimal solution by iteratively adjusting the positions of the particles.

Parameter Space Exploration:

The parameters of an ANN, such as learning rates, weights, and biases, collectively form a parameter space. PSO is employed to explore this parameter space intelligently. Each particle in the swarm represents a potential set of parameters for the ANN.

Initialization:

The PSO process begins with the initialization of a swarm of particles, each assigned a random position in the parameter space. The fitness of each particle, indicating its performance, is evaluated based on a predefined objective function, such as accuracy in the case of intrusion detection.

Velocity and Position Update:

Each particle adjusts its velocity and position based on its own experience (local best) and the collective experience of the swarm (global best). Velocity and position updates are determined by balancing exploration and exploitation to converge toward the optimal solution.

Objective Function Evaluation:

After each update, the fitness of particles is re-evaluated using the objective function. The objective function measures how well a particular set of parameters contributes to the desired outcome, such as accurate intrusion detection.

Iteration and Convergence:

The PSO algorithm iteratively refines the positions of particles, allowing them to converge toward the optimal solution. Convergence is achieved when the swarm settles into a region of the parameter space that corresponds to optimal ANN parameters.

Parameter Tuning for ANN:

The final positions of particles in the parameter space represent the optimized parameters for the ANN.

These optimized parameters are then used in training the ANN for intrusion detection.

The overall performance of the proposed model is compared with DT and KNN which is represented in Table 1.

Table 1. Performance Comparison

Method	Accuracy	Specificity	Sensitivity
K- Nearest Neighbor	85%	83%	86.5%
Decision Trees	80%	72%	82%
PSO+ANN	97.5%	95%	96%

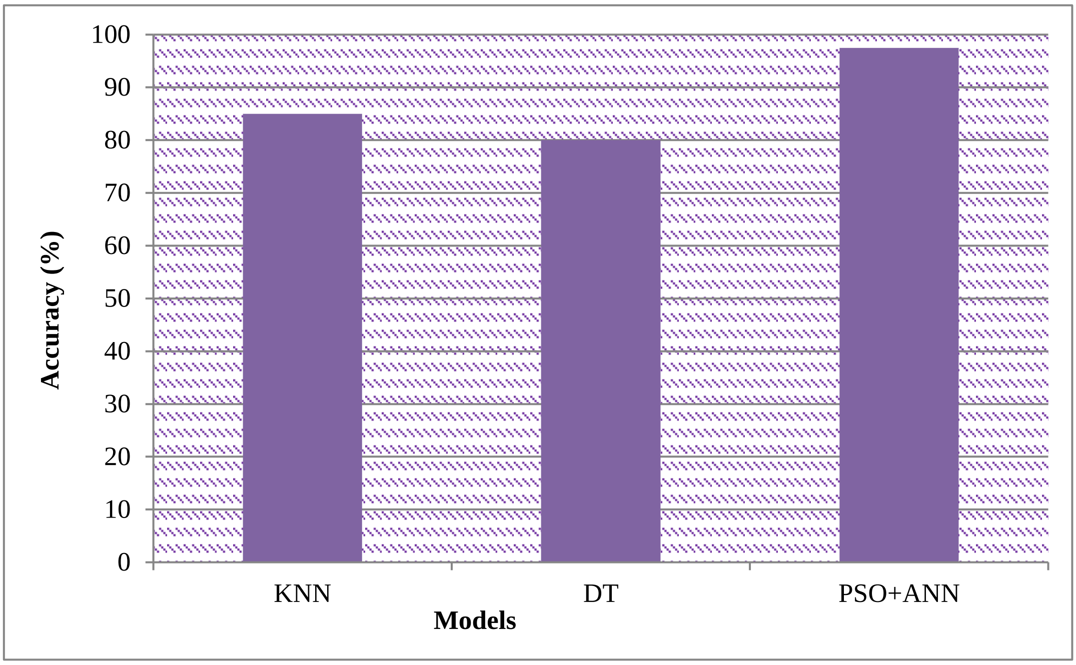

Fig. 2. Accuracy Result

The comparison of accuracy performance metrics among the conventional Decision Trees (DT) and K-Nearest Neighbors (KNN) models, and the innovative PSO-ANN is illustrated in Fig. 2. On the y-axis of the figure, various approaches depict their respective accuracy values, with the corresponding values arranged along the x-axis. The proposed ANN employs weight values for classification, resulting in increased accuracy. The outcomes underscore the superior accuracy of the proposed PSO-ANN framework, yielding an impressive 97.5%, surpassing the DT and KNN models, which achieve only 80% and 85%, respectively.

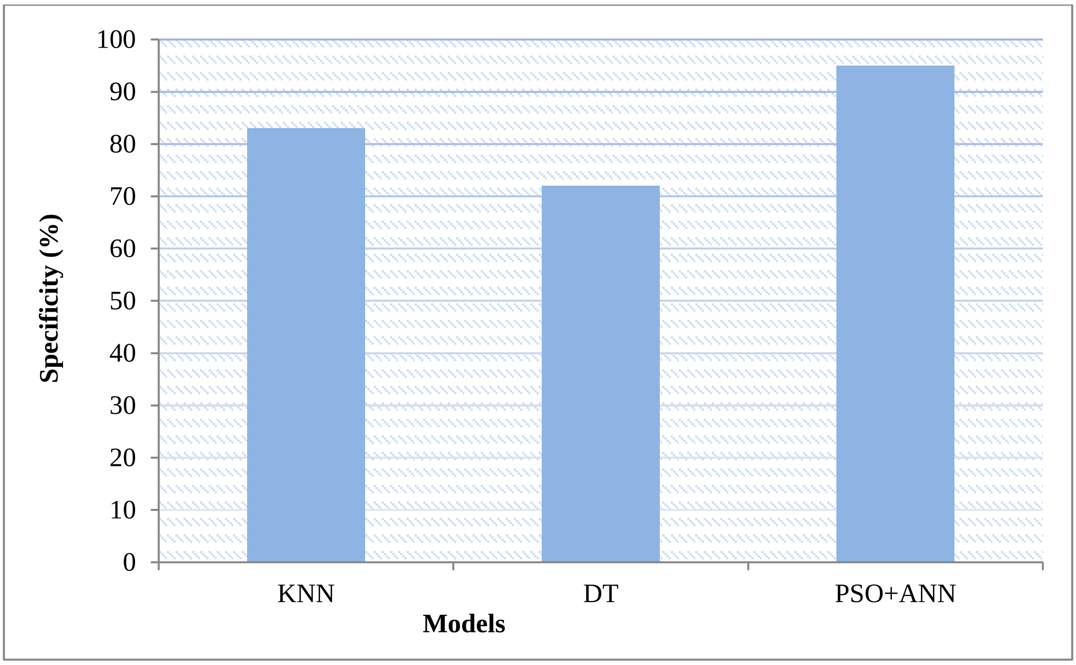

Fig. 3. Specificity Result

In Fig. 3, a performance comparison analyzes the specificity of the proposed PSO-ANN model against existing Decision Trees (DT) and K-Nearest Neighbors (KNN) models. The y-axis displays different approaches, while the x-axis presents accuracy values. Notably, the PSO-ANN model exhibits superior specificity at 95%, outperforming DT (72%) and KNN (83%). This emphasizes the efficacy of the proposed PSO-ANN approach in achieving more accurate and precise outcomes, showcasing its potential for robust applications in comparison to traditional DT and KNN methods.

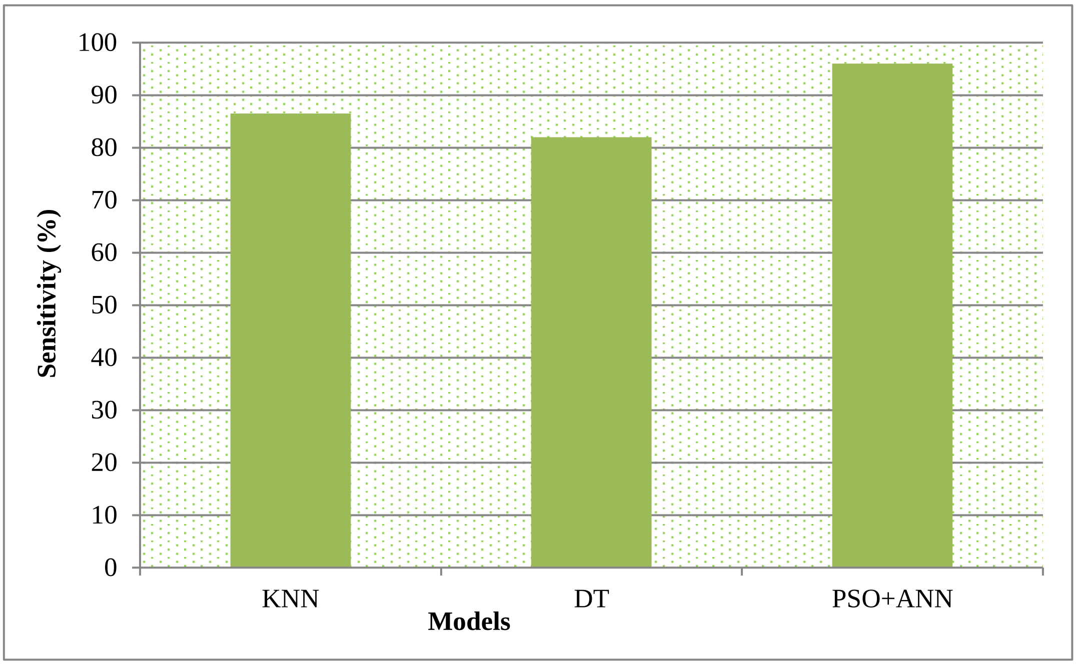

Fig. 4. Sensitivity Result

In Fig. 4, a performance comparison analyzes the sensitivity of the proposed PSO-ANN model against existing Decision Trees (DT) and K-Nearest Neighbors (KNN) models. The y-axis displays different approaches, while the x-axis presents accuracy values. Notably, the PSO-ANN model exhibits superior sensitivity at 96%, outperforming DT (82%) and KNN (86.5%). This emphasizes the efficacy of the proposed PSO-ANN approach in achieving more accurate and precise outcomes, showcasing its potential for robust applications in comparison to traditional DT and KNN methods.

6. Conclusion

In conclusion, this research introduces an innovative strategy to enhance Wireless Sensor Networks (WSNs) security by integrating Particle Swarm Optimization (PSO) with an Artificial Neural Network (ANN) for a robust Network Intrusion Detection System (NIDS). WSNs, constrained by resources and dynamic environments, face diverse security threats. The proposed system employs PSO to optimize ANN parameters, aiming to elevate intrusion detection accuracy and efficiency. PSO facilitates exploration of the ANN's parameter space, enabling the network to adapt to WSN characteristics and discern normal from malicious activities effectively. The study involves designing and implementing the PSO-based ANN model, followed by extensive evaluations of real-world WSN datasets from Kaggle. Results demonstrate the superior NIDS performance, exhibiting heightened accuracy, sensitivity, and specificity compared to conventional methods. The synergy between PSO and ANN contributes to a resilient and adaptive intrusion detection system tailored for resource-constrained WSNs. This research not only meets the imperative demand for reliable WSN security mechanisms but also lays the foundation for advancements at the intersection of optimization techniques and artificial intelligence in cybersecurity for wireless sensor environments. The proven success of the PSO + ANN method, outperforming KNN and decision trees, highlights its potential to fortify WSN security. As the field advances, these findings offer valuable insights for future research, shaping the landscape of optimization-driven artificial intelligence in addressing the evolving challenges of wireless sensor security.

References

[1] Arsalwad, G., More, S., Tiwari, A., Zade, R., & Kudale, K. (2023). Analyze And Forecast The Cyber Attacks Using Machine Learning Techniques. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(11), 2566-2569.

[2] Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023). Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. *Applied Sciences*, *13*(13), 7507.

[3] Ponnusamy, V., Yichiet, A., Jhanjhi, N. Z., & Almufareh, M. F. (2022). IoT Wireless Intrusion Detection and Network Traffic Analysis. *Computer Systems Science & Engineering*, *40*(3).

[4] Jhaveri, R. H., Revathi, A., Ramana, K., Raut, R., & Dhanaraj, R. K. (2022). A review on machine learning strategies for real-world engineering applications. *Mobile Information Systems*, *2022*.

[5] Muruganandam, S., Salameh, A. A., Pozin, M. A. A., Manikanthan, S. V., & Padmapriya, T. (2023). Sensors and machine learning and AI operation-constrained process control method for sensor-aided industrial internet of things and smart factories. *Measurement: Sensors*, *25*, 100668.

[6] Liu, J., and Zhu, L. (2021). Joint Resource Allocation Optimization of Wireless Sensor Network Based on Edge Computing. *Cognitive Computing Solutions for Complexity Problems in Computational Social System*, *2021*, Article ID 5556651, 1-11.

[7] Shreyanth, S. Prevention of cyberattacks in WSN and packet drop by CI framework and information processing protocol using AI and Big Data.

[8] Arshad, J., Azad, M. A., Mahmoud Abdellatif, M., Ur Rehman, M. H., & Salah, K. (2019). COLIDE: A collaborative intrusion detection framework for Internet of Things. *IET Networks*, *8*(1), 3-14.

[9] A.J. Malik, F.A. Khan. (2017). A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection. *Cluster Comput., 21*(2018), 667–680.

[10] Mojtahedi, A., Sorouri, F., Souha, A. N., Molazadeh, A., & Mehr, S. S. (2022). Feature selection-based intrusion detection system using genetic whale optimization algorithm and sample-based classification. *arXiv preprint arXiv:2201.00584*.

[11] Ramani, S., Rao, S. S., Latha, S., & Prasad, L. C. (2022). A Novel Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) and Random Artificial Neural Network Combined Gradient Descent (RANN-GD) Algorithm for WSN Security. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(4), 07-15.

[12] Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An enhanced intrusion detection model based on improved kNN in WSNs. *Sensors*, *22*(4), 1407.

[13] Xu, H., Przystupa, K., Fang, C., Marciniak, A., Kochan, O., & Beshley, M. (2020). A combination strategy of feature selection based on an integrated optimization algorithm and weighted k-nearest neighbor to improve the performance of network intrusion detection. *Electronics*, *9*(8), 1206.