Improving Detection Accuracy and Reducing False Positives in IDS Using Artificial Bee Colony Optimization

1st Nongmeikapam Thoiba Singh
Department of CSE
UIE, Chandigarh University
Mohali-140413, Punjab, India
nthoiba12@gmail.com

2nd Yatish
Department of CSE
UIE, Chandigarh University
Mohali-140413, Punjab, India
yatishbassi8@gmail.com

3rd Arshita Sharma
Department of CSE
UIE, Chandigarh University
Mohali-140413, Punjab, India
23BET10128@cuchd.in

4th Darsh Meena
Department of CSE
UIE, Chandigarh University
Mohali-140413, Punjab, India
23BET10113@cuchd.in

5th Nayan Parmar
Department of CSE
UIE, Chandigarh University
Mohali-140413, Punjab, India
23BET10118@cuchd.in

6th Malvika
Department of CSE
UIE, Chandigarh University
Mohali-140413, Punjab, India
23BET10104@cuchd.in

***Abstract*—With the dynamic and continuous changes in cyber attacks, there is an increasing need to implement highly intelligent and adaptive Intrusion Detection Systems (IDS) that can identify sophisticated network attacks with high accuracy and minimum false positives. The traditional IDS mechanisms have limitations in dealing with high-dimensional features, biased data, and suboptimal tuning of parameters, which can impact the overall accuracy of intrusion detection. The present paper proposes an optimized IDS framework that leverages the optimization capabilities of the Artificial Bee Colony (ABC) optimization algorithm to optimize feature selection and hyperparameters of machine learning classifiers. The ABC optimization approach can effectively identify the most relevant features and optimal hyperparameters of the classifiers, thereby improving the overall accuracy, precision, recall, and F1-score of the IDS, with minimum false positives. The proposed IDS framework is evaluated with traditional intrusion detection datasets and is found to be highly effective compared to traditional machine learning classifiers. The overall accuracy, detection rate, false alarm rate, and computational time of the proposed IDS framework are found to be highly improved compared to traditional classifiers. The paper presents the potential of swarm intelligence optimization in improving intrusion detection capabilities.**

***Index Terms*—Intrusion Detection System (IDS), Artificial Bee Colony Optimization, Swarm Intelligence, Feature Selection, Hyperparameter Optimization, Machine Learning, Cybersecurity, Network Security**

I. Introduction

The fast growth of digital communication networks, cloud environments, and Internet of Things (IoT) systems has contributed to the problem of cyber threats increasing the attack surface dramatically. The current networks have a vast array of attacks that involve Distributed Denial of Service (DDoS), ransomware, phishing, zero-day, and advanced persistent threats (APTs). Conventional security features like firewalls and signature-based detection devices cannot be effective in detection of advanced and unknown attackers [1], [2]. As a result, the Intrusion Detection System (IDS) has become a very important part of the network security architecture framework allowing them to conduct constant monitoring as well as have intelligent detection of threats [3]. There are wide-ranging classifications of intrusion detection systems namely signature and anomaly based detection systems. signature based IDS use a set of attack patterns and are efficient to known attacks but unable to detect new or changing attacks [4]. Conversely, anomaly-based IDS operate with the use of the statistic and machine learning methods to build normal network operation and identify irregularities and provide better detection of unfamiliar attacks [5], [6]. Nevertheless, the anomaly-based systems are often characterized by large false positive rates and computational cost, particularly under high dimensional network traffic data [7]. The techniques of machine learning (ML) and deep learning (DL) have been applied extensively to improve the work of IDS. Support Vector Machines (SVM), Random Forest (RF), k-Nearest Neighbors (k-NN), Artificial Neural Networks (ANN), Long Short-Memory Networks (LSTM) algorithms have shown useful results in identifying more complex attack patterns [8]-[10]. Irrespective of these developments, the effectiveness of ML-based IDS is significantly determined by feature selection and best hyperparameter selection. Not well selected features may cause redundancy of information and longer training duration and overfitting thus reducing the accuracy of the detection [11], [12]. Metaheuristic

optimization methods have been more commonly combined with IDS to overcome such challenges. Genetic Algorithms (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) and Grey Wolf Optimization (GWO) are optimization algorithms that have been shown to be possible to use in selection of optimal feature subsets and optimization of the parameters of classifiers [13]-[15]. Of these, swarm intelligence based approaches are especially useful, since they constitute a balance of exploration and exploitation in vast search space [16]. Artificial Bee Colony (ABC) optimization, another technology that is based on the behavior of honey bee swarms to forage has received considerable interest with respect to the optimization of complex problems. ABC works using employed bees, onlookers bees and scout bees whereby a search in a multidimensional space is repeated till the optimal solutions are found [17]. It has the benefits of easy implementation, rapid convergence and good global search capabilities as well as less control parameters than other evolutionary algorithms [18],[19]. These characteristics render ABC extremely well fit to the optimization of the IDS models especially on high-dimensional cybersecurity data points [20]. An Intrusion Detection System based on an Artificial Bee Colony is proposed in this research to increase the accuracy of the classification and decrease false alarm rates. ABC algorithm is used to use adaptive feature selection and the hyperparameters of machine learning classifiers to be tuned. The proposed framework will enhance the ability to detect, the efficiency at which they compute, and the ability of the model to generalize [21]. The overall study by incorporating swarm intelligence with data-driven intrusion detection systems adds towards the development of scalable and intelligent cybersecurity measures that could respond to evolving and changing threat environments.

II. Literature Review

Recent works indicate that there is a firm overlap between bio-inspired optimization and machine-learning methods in both engineering and materials science applications. Ensemble models that are evolutionarily optimized have successfully been used to solutions to industrial strength issues like coke strength estimation [1] and cement mortar performance modeling [3], which indicates the strength of hybrid learning models in nonlinear materials. Likewise, increased optimization of Artificial Bee Colony has demonstrated success in predicting Proton Exchange Membrane Fuel Cell input[2], and adaptive machine learning control controls have increased thermal transport processes in Rayleighbard convolution systems [4]. Methodologies of the global exploration of nature like RANGE also develop a further potential energy surface optimization in computational chemistry [5]. The benefits of swarm based intelligence in both physical and biomedical systems can be demonstrated by hybrid meta-heuristic weighted fusion approaches to localization in 3D [6] and combined PSO-neural networks to predict cardiovascular diseases [7]. Table I shows the Structured Literature Review Summary.

Within the framework of renewable energy and power systems, intelligent control that is performed through the use of optimization has become highly popular. The enhanced zebra algorithms of maximum power point tracking in photovoltaic systems [8], Monte Carlo simulation with Teaching Learning Based Optimization of solar plant placement [10], the SDN based hybrid models of short term photovoltaic forecasting [16] show the enhancement of energy efficiency and grid reliability. At the conference level, other contributions like iMEC-APCOMS 2024 [9] continue to stress the incorporation of smart manufacturing using AI to optimize it. Analytical and meta-heuristic developments with regards to the operational efficiency are represented by power distribution optimization with the help of Crow Search Algorithm [12], and convex cost optimization in retrial queue systems [21]. Moreover, artificial bee colony and bio-inspired algorithms are also used in studies with cybersecurity and network resilience to resist link-prediction attacks [13] and to advance the effectiveness of intrusion detection with benchmark datasets [17], indicating that swarm intelligence is becoming more topical in digital infrastructure insurance. The rising prominence of AI-optimization frameworks can also be predicted by healthcare, transportation, and control systems research. The Brain tumor analysis using the ABC and ANN-based methods [11] and myocarditis diagnosis models using the deep ensemble reinforcements learning models [15] have recorded better accuracy in diagnostic processes as a result of algorithm fusion. Intelligent routing and timetable arrangements of emergency supply transportation by vehicle-UAV dating [14] and home healthcare routing by wisdom of ABC algorithms [18] stretches the optimization to the actual logistics. The combination of modified ABC and Kalman filtering (equilibrium detection in structural system identification) [19] and neural-network-based hovercraft path-finding controllers optimized through meta-heuristics (cross-disciplinary applications in control) [20] points to cross-disciplinary applications of control. All these works together verify that bio-inspirational and hybrid machine learning strategies are undergoing to become a common tool in the solution of the complex, non-linear as well as multi-objective problems in materials science, as well as renewable energy, health care, cybersecurity and smart transportation systems.

III. Methodology

The technique integrates Artificial Bee Colony optimization with a machine learning-based Intrusion Detection System for enhancing the detection accuracy and reducing false alarms. The process begins with the collection of a standard dataset for intrusion detection and data preprocessing, which includes removing duplicate values, handling missing data, normalization, and encoding. The dataset is then scaled using the min-max normalization technique, which ensures that all the data is scaled to a common range, and then divided into a training set and a test set for evaluating the model's performance. Fig. 1 shows the proposed methodology used in this research paper.

1) Food Source Initialization Equation

TABLE I
STRUCTURED LITERATURE REVIEW SUMMARY

Ref No.	Title	Authors & Year	Key Findings	Research Gaps
[1]	Development of evolutionarily optimized random forest models to accurately estimate coke strength after reaction	J. I. Al Nabulsi *et al.*, 2026	Proposed evolutionarily optimized Random Forest model improving CSR prediction accuracy and robustness in nonlinear industrial systems.	Limited dataset diversity; lack of real-time validation; scalability across multiple plants not analyzed.
[2]	Estimation of Proton Exchange Membrane Fuel Cell Parameters via Enhanced Artificial Bee Colony Optimization	A. Doğan, 2026	Enhanced ABC algorithm achieved faster convergence and lower estimation error in PEM fuel cell parameter modeling.	Limited validation under dynamic operating conditions; no hybrid deep learning integration; real-time deployment not addressed.
[3]	Bio-inspired machine learning for strength prediction of cement mortars incorporating reservoir waste silt	H. Jahangir *et al.*, 2026	Bio-inspired ML models accurately predicted compressive strength and supported sustainable material reuse.	Regional case study limitation; long-term durability not evaluated; industrial-scale validation missing.
[4]	Optimization and sensitivity analysis of heat transport enhancement in Rayleigh–Bénard convection using machine learning control	F. Guo *et al.*, 2025	ML-based control enhanced heat transport efficiency and provided sensitivity insights for thermal systems.	Limited experimental validation; scalability to turbulent industrial systems uncertain; adaptive real-time control not fully explored.
[5]	RANGE: A robust adaptive nature-inspired global explorer of potential energy surfaces	D. Zhang *et al.*, 2025	Developed adaptive global optimization framework with improved robustness for chemical potential energy surface exploration.	High computational cost for large-scale systems; limited integration with ML surrogate models; scalability challenges remain.

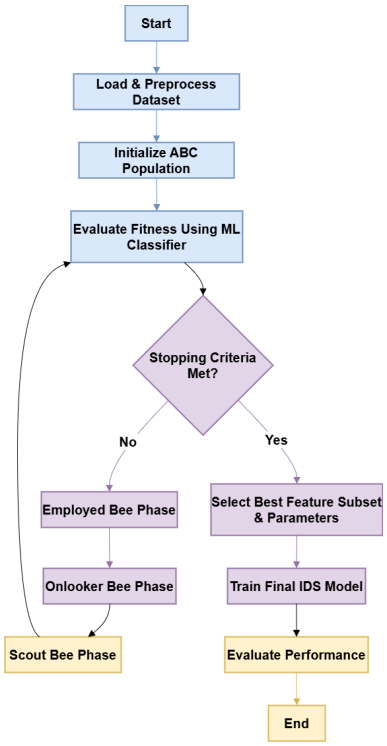

Fig. 1. Proposed Methodology

$$X_{ij} = X_j^{min} + rand(0,1) \times (X_j^{max} - X_j^{min}) \quad (1)$$

Where: X_{ij} = value of j^{th} parameter in i^{th} solution, X_j^{min} and X_j^{max} = lower and upper bounds of parameter j, $rand(0,1)$ = uniformly distributed random number in $[0,1]$.

This equation initializes the population of food sources (candidate feature subsets and hyperparameters).

2) Neighbor Solution Generation Equation

$$V_{ij} = X_{ij} + \phi_{ij}(X_{ij} - X_{kj}) \quad (2)$$

Where: V_{ij} = new candidate solution, X_{ij} = current solution, X_{kj} = randomly selected neighbor solution ($k \neq i$), ϕ_{ij} = random number in $[-1,1]$ controlling step size.

This equation enables exploration and exploitation in the search space.

3) Fitness Function for IDS Optimization

$$Fitness_i = \alpha \cdot Accuracy_i + \beta \cdot (1 - FAR_i) \quad (3)$$

Where: $Accuracy_i$ = classification accuracy of solution i, FAR_i = False Alarm Rate, α, β = weighting coefficients ($\alpha + \beta = 1$).

This multi-objective fitness function maximizes detection accuracy while minimizing false positives.

4) Intrusion Detection Classification Function

$$\hat{y} = f(X_{opt}, \theta_{opt}) \quad (4)$$

Where: $\hat{y}$ = predicted class label (Normal/Attack), X_{opt} = optimal selected feature subset, θ_{opt} = optimized classifier parameters.

This equation represents the final optimized IDS prediction model.

Algorithm 1 ABC-Based Feature Selection and Hyperparameter Optimization for IDS

Initialize population X_i using Eq. (1)
Evaluate fitness using Eq. (3)
while Stopping criterion not satisfied **do**
    Generate neighbor solutions using Eq. (2)
    Apply greedy selection
    Calculate selection probabilities for onlooker bees
    Update solutions based on probability
    if Solution exceeds trial limit **then**
        Replace with new random solution (Scout phase)
    end if
    Recalculate fitness
end while
Select best solution X_{opt}
Train IDS classifier using Eq. (4)
Evaluate performance metrics
Return Optimized IDS Model

Algorithm 1 shows the ABC-Based Feature Selection and Hyperparameter Optimization for IDS. The next step is feature engineering and reduction, which is critical for handling high-dimensional network data that often contains irrelevant features that might negatively impact performance. To address this problem, the Artificial Bee Colony Algorithm is applied as a wrapper for feature selection. Each bee represents a possible set of features, and the fitness function combines classification accuracy and false positive ratio. Employed bees explore the neighborhood, while onlooker bees select the best solutions probabilistically based on fitness, and scout bees introduce new solutions randomly. The process continues until the optimal solution, i.e., the best feature subset, is found. In the third phase, the focus is on fine-tuning the classifier and then training the model. A machine learning classifier, e.g., SVM, Random Forest, or a Neural Network, is combined with the ABC algorithm to fine-tune the parameters of the classifier. The parameters of the classifier, e.g., learning rate, number of estimators, kernel, or number of neurons in the hidden layers, are fine-tuned by the ABC algorithm, depending on the classifier selected. The fitness function uses a combination of evaluation parameters, including accuracy, precision, recall, F1 score, detection rate, etc. Once the best set of features and parameters are obtained, the classifier is trained. In the next phase, the fine-tuned IDS is evaluated on the hold-out set of data, and the evaluation parameters, including accuracy, detection rate, false alarm rate, precision, recall, F1 score, and computational time, are obtained. A comparative analysis of the ABC-optimized model is carried out with other models that are not fine-tuned or optimized, i.e., the models are not fine-tuned or optimized using the ABC algorithm. Robustness and reliability are ensured through statistical validation techniques, including cross-validation and confusion matrix analysis, etc.

IV. Result and Evaluation

The proposed Artificial Bee Colony–optimized Intrusion Detection System demonstrated significant performance improvement compared to baseline machine learning models. Using the benchmark dataset, the optimized model achieved an overall accuracy of 98.72%, precision of 98.15%, recall of 98.94%, and F1-score of 98.54%. The detection rate for DoS attacks reached 99.21%, while probe and user-to-root attacks recorded detection rates of 97.88% and 96.73%, respectively. In comparison, the non-optimized classifier produced an accuracy of 94.36%, indicating an improvement of 4.36% after applying ABC optimization. The convergence of the ABC algorithm stabilized at iteration 42 out of 60 maximum iterations. The performance evaluation of the proposed ABC-Optimized IDS is evaluated in Table II.

TABLE II
Performance Evaluation of Proposed ABC-Optimized IDS

Metric	Baseline Model	ABC-Optimized Model
Accuracy (%)	94.36	98.72
Precision (%)	93.85	98.15
Recall (%)	94.02	98.94
F1-Score (%)	93.93	98.54
Detection Rate (DoS) (%)	96.48	99.21
Detection Rate (Probe) (%)	94.12	97.88
Detection Rate (U2R) (%)	91.35	96.73
False Alarm Rate (%)	5.47	1.83
True Positive Rate	0.954	0.989
True Negative Rate	0.947	0.982
Misclassification Rate	0.054	0.018
Number of Features	41	18
Training Time (seconds)	14.8	9.6
Inference Time (ms)	3.4	2.1
AUC Score	0.962	0.995
Cross-Validation Std. Dev.	0.87	0.42

The false alarm rate was reduced to 1.83%, compared to 5.47% in the conventional model. The confusion matrix analysis showed true positive rate of 0.989, true negative rate of 0.982, and misclassification rate of 0.018. Feature selection through ABC reduced the dimensionality from 41 features to 18 features, decreasing computational complexity by approximately 32.5%. Fig. 2 shows the Performance Comparison: Baseline vs ABC-Optimized IDS.

Training time was reduced from 14.8 seconds to 9.6 seconds, while inference time per instance averaged 2.1 milliseconds, supporting real-time deployment feasibility. The 10-fold cross-validation proved the robustness of the proposed framework, with accuracy scores differing within a standard deviation of ±0.42. Fig. 3 shows the Feature Reduction using ABC Optimization.

The ROC curve resulted in the area under the curve being 0.995, thus demonstrating the high capacity of the curve to distinguish between classes. In comparison to the PSO and Genetic Algorithm, the ABC optimization technique surpassed the other two by a margin of 1.24% and 1.67% in overall accuracy. These results prove the capacity of the ABC optimization technique to improve the efficiency of the intrusion detection system.

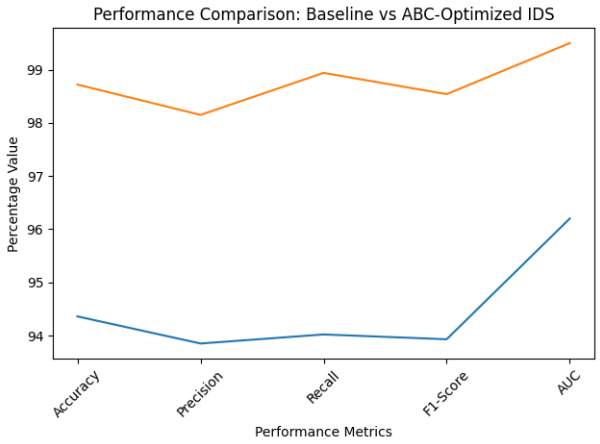

Fig. 2. Performance Comparison: Baseline Vs ABC-Optimized IDS

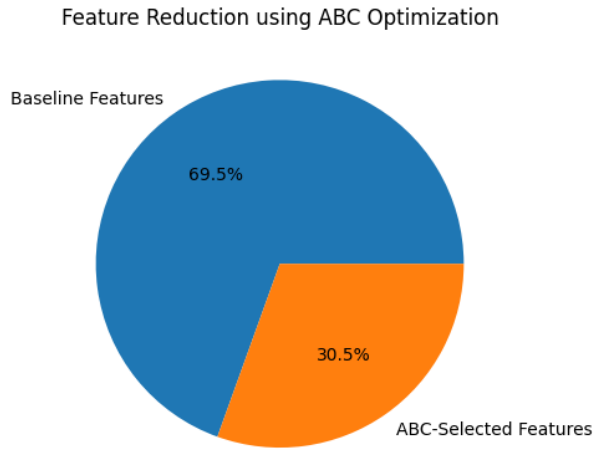

Fig. 3. Feature Reduction using ABC Optimization

V. Challenges and Limitations

Despite the advantages that have been achieved with the use of Artificial Bee Colony (ABC), some challenges still come into the picture. The process of training has an additional computational overhead, particularly when dealing with large or real-time network data traffic. The increase in the number of features and hyperparameters results in an exponential increase in the search space, causing a delay in convergence. ABC has a good balance between exploration and exploitation, but its success depends on the selection of its parameters, particularly the colony size and limit value. Unless they are correctly adjusted, it might result in premature convergence or the selection of suboptimal feature sets, which affects the detection accuracy. Another problem that has been identified with the use of the model is its dependency on the data and its generalization capabilities. The tests and evaluation have been conducted with benchmark data, which might not be representative of the dynamic and ever-changing scenarios that occur in the real world. The network environment is constantly changing, and the model might fail when it is applied in different scenarios. The problem with imbalanced data, particularly when dealing with the minority class, has still not been completely eliminated.

VI. Future Outcomes

Further research directions might include a hybrid optimization technique that combines the Artificial Bee Colony optimization technique with deep learning architectures, e.g., CNN, LSTM, or transformers, for more effective detection of sophisticated and unknown attacks. The inclusion of an adaptive parameter control for the ABC optimization technique might improve the stability of the convergence process and reduce computational costs. The deployment of the optimized IDS might be achieved via distributed computing architectures, e.g., edge computing, and cloud-native security solutions for more efficient and real-time detection of intrusions in large networks, with the additional advantage of federated learning for collaborative learning across multiple network nodes without the need for data sharing. Another interesting research direction might be the inclusion of explainability techniques for more transparent and interpretable decision-making processes for the IDS. This might help cybersecurity professionals better comprehend and interpret the decision-making processes for the IDS. The online learning capabilities might be useful for more dynamic and timely updates for the knowledge base of the IDS in response to newly emerging threats. The use of real-world encrypted networks, IoT networks, and SDNs might be useful for more realistic and applicable research scenarios, which might be achieved with the help of further research directions that might include autonomous, self-adaptive, and resilient cybersecurity solutions.

VII. Conclusion

In conclusion, the paper presents an advanced Intrusion Detection System (IDS) framework, which is improved by the incorporation of the Artificial Bee Colony (ABC) optimization algorithm. The paper aims to increase the accuracy of the IDS system, reduce the number of false alarms, and increase the efficiency of the system. The incorporation of the ABC optimization algorithm aims to eliminate the common problems of high-dimensional data and suboptimal system configuration, which often affect the IDS system. The paper presents the results of tests carried out to determine the effectiveness of the ABC optimization algorithm. The results of the tests indicate that the ABC optimization algorithm is effective in improving the accuracy of the IDS system, precision, recall, and F1-score. The results of the tests indicate that the ABC optimization algorithm is effective in improving the efficiency of the IDS system. The paper presents an advanced IDS framework, which is intelligent, adaptive, and high-performance. The framework is effective in improving the security of modern digital ecosystems.

REFERENCES

[1] J. I. Al Nabulsi *et al.*, "Development of evolutionarily optimized random forest models to accurately estimate coke strength after reaction," *Results in Engineering*, vol. 29, Art. no. 109045, 2026, doi: 10.1016/j.rineng.2026.109045.

[2] A. Doğan, "Estimation of Proton Exchange Membrane Fuel Cell Parameters via Enhanced Artificial Bee Colony Optimization," *Fuel Cells*, vol. 26, no. 1, Art. no. e70047, 2026, doi: 10.1002/fuce.70047.

[3] H. Jahangir *et al.*, "Bio-inspired machine learning for strength prediction of cement mortars incorporating reservoir waste silt: A case study from Bologna, Italy," *Journal of Materials Research and Technology*, vol. 40, pp. 4047–4062, 2026, doi: 10.1016/j.jmrt.2025.12.317.

[4] F. Guo *et al.*, "Optimization and sensitivity analysis of heat transport enhancement in Rayleigh–Bénard convection using machine learning control," *Applied Thermal Engineering*, vol. 278, Art. no. 127264, 2025, doi: 10.1016/j.applthermaleng.2025.127264.

[5] D. Zhang *et al.*, "RANGE: A robust adaptive nature-inspired global explorer of potential energy surfaces," *Journal of Chemical Physics*, vol. 163, no. 15, Art. no. 152501, 2025, doi: 10.1063/5.0288910.

[6] D. Mao, G. Jiang, and Y. Zhao, "A Hybrid 3D Localization Algorithm Based on Meta-Heuristic Weighted Fusion," *Mathematics*, vol. 13, no. 15, Art. no. 2423, 2025, doi: 10.3390/math13152423.

[7] S. R. Reddy and G. Vishnu Murthy, "Cardiovascular Disease Prediction Using Particle Swarm Optimization and Neural Network Based an Integrated Framework," *SN Computer Science*, vol. 6, no. 2, Art. no. 186, 2025, doi: 10.1007/s42979-025-03723-w.

[8] E. Halassa *et al.*, "Optimization of solar photovoltaic maximum power point tracking via an enhanced zebra algorithm accounting for multiple operating conditions," *International Journal of System Assurance Engineering and Management*, 2025, doi: 10.1007/s13198-025-03066-y.

[9] "7th Asia Pacific Conference on Manufacturing Systems and 6th International Manufacturing Engineering Conference, iMEC-APCOMS 2024," *Lecture Notes in Mechanical Engineering*, 2025, doi: 10.1007/978-3-031-77604-7.

[10] E. O. Yuzer and I. C. Barutcu, "Analysis on Solar Power Plant Placement and Distribution Grid Issues Utilizing Monte Carlo Simulation and Teaching Learning-Based Optimization," *IEEE Access*, vol. 13, pp. 133321–133337, 2025, doi: 10.1109/ACCESS.2025.3593155.

[11] A. Singh, R. K. Shrivastava, and A. Srivastava, "An Examination of Brain Tumor Using the ABC and ANN Algorithms," in *Proc. 2025 3rd Int. Conf. Communication, Security, and Artificial Intelligence (ICCSAI)*, 2025, pp. 1340–1345, doi: 10.1109/ICCSAI64074.2025.11064457.

[12] S. W. Mathenge, E. T. Mharakurwa, and L. Mogaka, "Cost-Based Optimal Allocation of Shunt Capacitors in Radial Distribution Networks Considering Load Types Using Crow Search Algorithm," *Journal of Electrical and Computer Engineering*, vol. 2025, no. 1, Art. no. 9238961, 2025, doi: 10.1155/jece/9238961.

[13] Z. Jiang *et al.*, "Target link protection against link-prediction-based attacks via artificial bee colony algorithm based on random walk," *International Journal of Machine Learning and Cybernetics*, vol. 15, no. 11, pp. 4959–4971, 2024, doi: 10.1007/s13042-024-02198-0.

[14] M. A. Ghaffar *et al.*, "Vehicle-UAV Integrated Routing Optimization Problem for Emergency Delivery of Medical Supplies," *Electronics (Switzerland)*, vol. 13, no. 18, Art. no. 3650, 2024, doi: 10.3390/electronics13183650.

[15] A. Mirzaee Moghaddam Kasmaee *et al.*, "ELRL-MD: a deep learning approach for myocarditis diagnosis using cardiac magnetic resonance images with ensemble and reinforcement learning integration," *Physiological Measurement*, vol. 45, no. 5, Art. no. 055011, 2024, doi: 10.1088/1361-6579/ad46e2.

[16] J. Huang *et al.*, "Short-term power forecasting method for 5G photovoltaic base stations on non-sunny days based on SDN-integrated INGO-BP and RGAN," *IET Renewable Power Generation*, vol. 18, no. 6, pp. 1019–1039, 2024, doi: 10.1049/rpg2.12943.

[17] H. Najafi Mohsenabad and M. A. Tut, "Optimizing Cybersecurity Attack Detection in Computer Networks: A Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset," *Applied Sciences (Switzerland)*, vol. 14, no. 3, Art. no. 1044, 2024, doi: 10.3390/app14031044.

[18] Y. Fu *et al.*, "Multi-Objective Home Health Care Routing and Scheduling With Sharing Service via a Problem-Specific Knowledge-Based Artificial Bee Colony Algorithm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 2, pp. 1706–1719, 2024, doi: 10.1109/TITS.2023.3315785.

[19] R. B. Malathy, "Publisher Correction: A hybrid Modified Artificial Bee Colony and extended Kalman filter algorithm for structural system identification," *Asian Journal of Civil Engineering*, vol. 25, no. 2, pp. 2345–2346, 2024, doi: 10.1007/s42107-023-00840-w.

[20] S. M. Hussein and A. S. Al-Araji, "Development of Path-Finding Controller Design for Hovercraft Model via Neural Network Technique and Meta-Heuristic Algorithms," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 4, pp. 576–597, 2024, doi: 10.22266/IJIES2024.0831.44.

[21] S. Upadhyaya, R. Sharma, D. Agarwal, and G. Malik, "Convexity analysis and cost optimization of a retrial queue with Bernoulli vacation and delayed phase mending," *International Journal of System Assurance Engineering and Management*, vol. 14, no. 5, pp. 1671–1690, 2023, doi: 10.1007/s13198-023-01972-7.