SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I9P113

Volume 12 Issue 9, 153-161, September 2025

Original Article

Hybrid Metaheuristic-Driven Intrusion Detection System Using Opto-Romar Swarm Bee Genesis Optimization on IoT Network Data

Swetha A[1], Ramesh Sekaran[2] , Annamalai S[3]

[1,2,3]*Department of Computer Science and Engineering, JAIN (Deemed- to-be- University), Bangalore, Karnataka, India.*

[1]*Corresponding Author : swethaashok28@gmail.com*

Received: 13 July 2025 Revised: 15 August 2025 Accepted: 14 September 2025 Published: 29 September 2025

Abstract *- The Internet of Things (IoT) devices have rapidly grown in numbers, posing critical threats in the process of securing networks against emerging cyber-attacks. Traditional Intrusion Detection Systems (IDS) suffer from low accuracy, are not flexible and are inefficient in handling massive multidimensional IoT data. To mitigate these shortcomings, the study presents a new hybrid metaheuristic-based IDS system that combines Cat-Scale normalization technique, the feature selection algorithm: Mutualk-Best, the optimization technique Opto-Romar Swarm Bee Genesis and the hyperparameter optimization algorithm: Evalmax Hyper Net. The framework is developed to provide a balanced representation of features, minimize redundancy, enhance convergence, and learn dynamic parameters to provide robust intrusion detection. Experimental results on the IoT-IDS dataset show the effectiveness of the proposed work. The framework recorded 95% accuracy, 97% precision, 98.6% recall and 98.4% F1-score with an AUC of 0.9999, utilizing better results compared to other techniques of IDS like BESO-HDL and Modified Isolation Forest. These findings support that the combination of swarm intelligence and genetic algorithms, along with adaptive tuning, can present a better detection performance with the ability to scale in highly complex IoT environments. The results indicate the framework as a promising future-proof IDS solution. Future work will consider the deployment of real-world IoT to resource-limited devices, robustness against adversarial attack, and variants to edge and mobile computing tasks.*

Keywords *- Cat-scale normalization, Hyperparameter tuning, Intrusion Detection System, IoT security, Metaheuristic optimization, Mutual-best, Opto-Romar Model.*

1. Introduction

The high rate of growth of the Internet of Things (IoT) device attractiveness has boosted connectivity in various fields like health, transportation, and industrial sectors over the same period; however, the cross-sectoral growth has also escalated the likelihood of cyber-attacks. Traditional Intrusion Detection Systems (IDS) are characterized with a large number of false positives, poor flexibility to new threats, and are computationally inefficient to handle the high-dimensional and heterogeneous data that is common in IoT networks. There are a few machine learning and optimization-based IDS models that have been built, but few of them have specific coverage regarding the exploration of the algorithms, or the overall coverage of features, as well as scalability in an IoT setting. In addition, previous methods do not typically make use of adaptive hyperparameter tuning schedules, which have the detrimental side effects of open a model to overfitting and a lack of generalisability. This leaves a lot of research gaps in terms of the design of an IDS framework that is precise, efficient and flexible in terms of resource-constrained IoT systems. The outlined problem is solved by the current study proposing a hybrid IDS model that involves feature selection, optimization and adaptive hyperparameter tuning.

This work has four novel contributions. A novel hybrid optimization model, Opto-Romar Swarm Bee Genesis, which integrates Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC) and Genetic Algorithm (GA) algorithms, is also presented and provides a more consistent balance between global exploration and local exploitation. Second, giving further consideration to ensuring the interpretability of the feature selection, there will be a new feature selection approach introduced, called Mutualk-Best, which is based on the combination of mutual information with k-means clustering to provide enhanced redundancy reducing and interpretability. Third, a two-fold normalization algorithm known as Cat-Scale is implemented to support both categorical and numerical IoT features and also speed up convergence and stabilize the classification process. Lastly, a

dynamic hyperparameter optimization framework, Evalmax Hyper Net, is introduced that adapts hyperparameters in response to a variety of metrics to make the IDS more robust and high-performance in various attack scenarios.

The main aim of the research is as follows:

- To extract the IoT-IDS dataset as well as process it effectively and prepare it towards IDS modeling.
- To normalize the features on the Cat-Scale to achieve similar characteristics instead of the heterogeneous data.
- To introduce the method of Mutualk-Best in optimally selecting features using mutual information and clustering.
- The Opto-Romar Swarm Bee Genesis model has been designed to combine PSO, Bee Colony, and the history of those Genetic Algorithms to train effectively.
- Evalmax HyperNet is used to carry out dynamic hyperparameter optimisation and enhanced generalisation.
- To assess the competency of the proposed IDS in terms of accuracy, precision, recall, and F1-score.
- Clear objectives should be established 1, listed as bullet points to give clarity.

The current studies in the field of IoT intrusion detection point to the significant role of associating optimization and machine learning. To give an example, previous studies have used Deep Neural Networks in conjunction with Chicken Swarm Optimization or Grey Wolf Optimization in ensemble modeling. Other work has presented more advanced metaheuristics, including the Binary Spider Wasp Optimizer, the well-known hybrid autoencoder feature selection using the modified PSO, or the derivation of DDoS attacks through the Snake Optimizer together with deep learning ensembles. These approaches have yielded encouraging results, but in many cases require excessive computational time, cannot be generalized across data sets, or cannot avoid getting stuck at local optima. Most of them lack adaptive tuning of hyperparameters, thus they have lower responses to novel or previously unseen attack patterns.

The presented methodology addresses the above limitations by integrating the normalization of features, smart feature selection, hybrid metaheuristics, and adaptive parameter tuning in a single algorithm. The experimental data on the IoT-IDS dataset indicate this approach significantly improves accuracy, precision, recall, and F1-score over the state-of-the-art techniques, with a low false positive rate.

This development demonstrates that integrating swarm intelligence, genetic operators, and adaptive tuning mechanisms is capable of generating an IDS framework that is not only highly performance but also scalable to the real-world IoT space. The rest of the paper is structured in the following way. Section 2 points out a summary of similar works and identifies their weaknesses. Section 3 provides the methodology proposed, including preprocessing, feature selection, training and optimization. Section 4 describes the experimental setup and performance measures. Section 5 provides a discussion of the results and a comparison with the existing methods. The last Section 6 summarizes the paper and sets future research directions.

2. Related works

Recent works have increasingly focused on combining deep learning with metaheuristic optimization to enhance IoT intrusion detection. In [9], the authors proposed a structure of anomaly detection by using a DNN and a Chicken Swarm Optimization (CSO) algorithm on IoT networks. The DNN has proven to be effective enough in a variety of fields, due to its property to draw prominent characteristics at various levels of abstraction out of unrefined input data. Deep learning Deep learning is a type of machine learning that is limited to huge descriptions with significant tiers of abstraction. A new method of Collective learning, based on the Grey Wolf Optimization (GWO) algorithm, is introduced in [10]. Classifiers used in the ensemble were a multilayer perceptron, K-nearest neighbors, a random forest, and a decision tree.

The ensemble learning paradigm of GWO has been applied to two publicly available datasets (BoT-IoT and UNSW-NB15). The article published in [11] adds the Improved Binary Spider Wasp Optimizer (IBSWO) to optimize feature selection, which constitutes a method of benchmarking the Spider Wasp Optimizer and genetic algorithm operations such as flat crossover. The tool was employed to test with some real-world datasets to demonstrate efficiency. The hybrid feature selection method developed by the authors of [12] was the HAEMPSO, where a modified PSO was used.

The Deep Neural Network (DNN) was used as the paired classifier for the hybrid approach. The adjusted inertia weight was used in optimizing the parameters of PSO and the model. The mechanism was experimented on BoT-IoT and UNSW-NB15 data, and it proposed the possibility of IoT usage. In the original procedure presented in [13] called DDAD-SOEL, attention was given to the automatic identification of DDOS attacks, where the Seagull Optimization (SO) algorithm was used to select the best feature combination, and the ensemble composed of DBN and 2 variations of LSTM (LSTM and BiLSTM).

In [14], the authors introduced the improved variation of the optimisation approach called the Grey Wolf Optimization (GWO). To satisfy the need, the proposed framework adopted a combined filter and the wrapper methods at the time of initialization so that the relevant features could be ensured to be selected earlier. The ELM classification was also utilized, whereby all parameters were optimized using the GWO.

The framework's effectiveness was demonstrated compared with other metaheuristic searching on the datasets of UNSW-NB15. In [15], the hybrid optimization approach was proposed to classify the mass-scale intrusion datasets to maximize the detection and minimize the false positives. In [16], it is proposed that a way to make (IoT) based Wireless Sensor Networks (WSNs) more secure is the implementation of the "Red Kite Optimization Algorithm Average Ensemble Intrusion Detection model (RKOA-AEID)". The particular approach used was the min-max normalization of data after preprocessing, the RKOA to choose features and the average ensemble classifier detection. The final model hyperparameters were also optimized a second time through the LCWOA. Last, [17] suggested the Planet Optimization with Deep CNN LWID. It focuses specifically on the resource constrained IoT scenarios, and has two parts: detection of attacks with the help of DCNN, and optimizing the hyperparameters with the use of the Planet Optimization (PO) algorithm, which provides the desired level of accuracy in computationally tractable contexts [18, 19].

Table 1. Comparative analysis of related works on IoT intrusion detection

Ref	Optimization Technique	Classifier(s) Used	Dataset(s)	Key Contribution
[9]	Chicken Swarm Optimization (CSO)	Deep Neural Network (DNN)	IoT Networks	Anomaly detection using DNN+CSO; leveraged DNN's ability for feature abstraction
[10]	Grey Wolf Optimization (GWO)	MLP, KNN, RF, DT (Ensemble)	BoT-IoT, UNSW-NB15	Collective learning ensemble with GWO for improved detection
[11]	Improved Binary Spider Wasp Optimizer (IBSWO)	Feature Selection (Benchmark vs GA)	Real-world datasets	Enhanced feature selection with IBSWO and GA operations
[12]	Hybrid Adaptive Evolutionary Modified PSO (HAEMPSO)	DNN	BoT-IoT, UNSW-NB15	Hybrid PSO with adjusted inertia weight; paired with DNN for classification
[13]	Seagull Optimization (SO)	DBN, LSTM, BiLSTM	IoT DDoS Detection	DDAD-SOEL framework for automated DDoS attack detection
[14]	Improved Grey Wolf Optimization (GWO)	Extreme Learning Machine (ELM)	UNSW-NB15	Hybrid filter-wrapper feature selection + GWO-based parameter optimization
[15]	Hybrid Optimization	Not specified	Large-scale intrusion datasets	Maximized detection accuracy, minimized false positives
[16]	Red Kite Optimization Algorithm (RKOA) + LCWOA	Average Ensemble Classifier	WSN datasets	RKOA-AEID framework with min-max normalization and feature selection
[17]	Planet Optimization (PO)	Deep CNN	IoT (resource-constrained)	LWID model combining DCNN detection + PO-based hyperparameter tuning

3. Methodology

This method proposes an intelligent intrusion detection framework, designed specifically for IoT environments, and it incorporates DL and advanced feature selection to increase the detection performance and accuracy. This method aims to improve the limitations of traditional security mechanisms in resource-limited IoT networks. The overall structure of the research is illustrated in Figure 1.

3.1. Dataset Collection and Preprocessing

Initially, we collect the data from the Kaggle dataset name "IoT dataset for Intrusion Detection Systems (IDS)". To ensure consistent representation of features in the IoT dataset, Cat-Scale normalization is implemented. This technique handles both categorical and numerical attributes, making them suitable for downstream learning algorithms.

It combines min-max scaling for numerical features with probability-based encoding for categorical variables. The Cat-Scale normalization process can be defined with the following equations:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

X is the original numerical feature value, X_{min} and X_{max} are the minimum and maximum values of that feature in the dataset, X' Is the scaled value in the range [0, 1]?

$$C' = \frac{f(C)}{N} \quad (2)$$

Where the C is a categorical value from a feature, $f(C)$ is the frequency count of category C in the dataset, N is the total number of records, C'Represents the encoded value for the categorical feature.

This dual approach ensures that all features, regardless of their original type, are normalized into a uniform scale. This improves convergence speed during model training and avoids bias from high-magnitude attributes, enabling better overall classification performance.

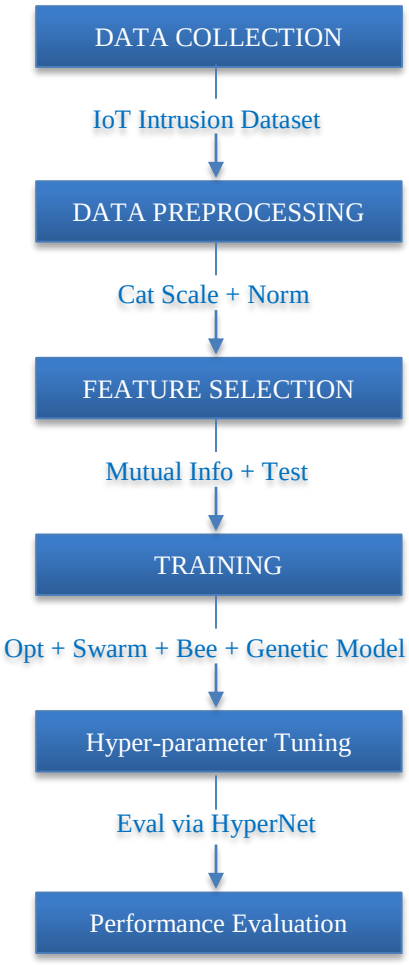

Fig. 1 Schematic representation of the suggested methodology

3.2. Feature Selection

Following preprocessing, the Mutualk-Best method is proposed for optimal feature selection by integrating Mutual Information (MI) with k-means clustering. This hybrid approach enhances the interpretability and discriminative power of selected features by prioritizing attributes that offer high relevance to the target class while ensuring minimal redundancy among themselves. The method begins by computing the mutual information between each feature and the class label to estimate its contribution toward classification. The mutual information between a feature F and the class label Y is given by:

$$MI(F_i, Y) = \sum_{f \in F_i} \sum_{y \in Y} P(f, y). \log\left(\frac{P(f,y)}{P(f).P(y)}\right) \quad (3)$$

Where F_i Represents the i-th feature, Y denotes the class label, $P(f, y)$ is the joint probability of feature value f and class y, $P(f)$ and $P(y)$ are the marginal probabilities of the feature and class label, respectively. This computation highlights the dependency between feature and label, guiding initial ranking. Subsequently, the top-ranked features are clustered using k-means clustering, grouping features based on their statistical similarity (e.g., correlation or Euclidean distance). Within each cluster, the most representative feature-i.e., the one closest to the cluster centroid-is selected. This step is mathematically formulated as:

$$Best(C_j) = arg\ arg\ ||F - \mu_j\ || \quad (4)$$

Where C_j Is the $j-th$ cluster of features, μ_j Is the centroid of the cluster C_j, $||F - \mu_j||$is the distance between feature F and the centroid. The final selected feature set, termed Mutualk-Best, contains highly informative, non-redundant features that balance relevance and uniqueness, thus improving the training phase's performance and reducing computation time.

After selecting the optimal feature subset using the Mutualk-Best approach, the training phase utilizes a novel hybrid metaheuristic optimization model named the Opto-Romar Swarm Bee Genesis Model. This model synergizes the strengths of "Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Genetic Algorithm (GA)" to achieve global convergence, adaptive learning, and exploration-exploitation balance in model training. The first component, PSO, simulates social behavior where particles (solutions) adjust their position based on personal and global best experiences. The position update of a particle is given by:

$$v_i^{(t+1)} = w.v_i^{(t)} + c_1.r_1.\left(p_i - x_i^{(t)}\right) + c_2.r_2.\left(g - x_i^{(t)}\right) \quad (5)$$

Where $v_i^{(t)}$ Is the velocity of particle i at iteration t, w is the inertia weight balancing exploration and exploitation, c_1 and c_2 are cognitive and social coefficients, r_1 and r_2 are random numbers in [0, 1], p_i Is the personal best position of particle i, g is the global best position, $x_i^{(t)}$ is the current position of the particle.

$$x_i^{(t+1)} = x_i^{(t)} + v_i^{(t+1)} \quad (6)$$

This equation updates the particle's position using the newly computed velocity. The Artificial Bee Colony (ABC) mechanism introduces a foraging strategy with employed, onlooker, and scout bees to enhance local exploration. The new solution generation by employed bees is modeled as:

$$v_{ij} = x_{ij} + \phi_{ij}.(x_{ij} - x_{kj}) \quad (7)$$

v_{ij} is the new solution for feature j of bee i, x_{ij} is the current solution, x_{kj} is a randomly selected neighbor, ϕ_{ij} It is a random number in $[-1, 1]$ controlling the perturbation strength. For global exploration and diversity, the Genetic Algorithm (GA) is integrated using crossover and mutation operations. The uniform crossover operation combines two parent solutions as follows: Equation (4):

$$Child_j = \{P1_j, if\ r\ and() < 0.5\ P2_j, \qquad otherwise \quad (8)$$

Where $Child_j$ is the j-th feature of the child solution, $P1_j$, $P2_j$ are the j-th features from parent 1 and 2, $rand()$ is a random number generator for selection. Mutation introduces diversity by flipping or modifying feature values:

$$x_j^{new} = \{x_j + \delta \; if \; r \; and() < p_m \; x_j, \qquad otherwise \qquad (9)$$

Where x_j^{new} Is the mutated feature, δ, a small mutation value (random perturbation), p_m Is the mutation probability? These combined mechanisms form the Opto-Romar model, where PSO contributes global best learning and direction tracking.

ABC adds exploitative local search using bee movement, and GA introduces adaptive diversity through crossover and mutation. This hybrid model is designed to escape local minima, accelerate convergence, and optimize model parameters for better classification accuracy during training on the intrusion detection dataset. To further optimize the performance of the trained intrusion detection model, the Evalmax Hyper Net is introduced as a dynamic hyperparameter tuning framework. It evaluates a network of possible hyperparameter combinations and selects the configuration that maximizes the model's performance based on a composite fitness function.

This method leverages performance metrics and adapts to the behavior of the model across validation folds. The composite evaluation function used to guide the search is defined as:

$$Eval_{Score} = \alpha.Acc + \beta.F1 + \gamma.(1 - FPR) \qquad (10)$$

Where $Eval_{Score}$ Is the evaluation score for a given hyperparameter set, Acc is the model accuracy, $F1$ is the F1-score, FPR is the false positive rate, α, β, γ are weight coefficients satisfying $\alpha + \beta + \gamma = 1$, and are set based on model priorities. The hyperparameter update in the Evalmax Hyper Net is based on the highest-ranked configurations evaluated so far. It uses a reward-penalty mechanism to refine search:

$$\theta^{(t+1)} = \theta^{(t)} + \eta.\nabla Eval_{Score}(\theta) \qquad (11)$$

Where $\theta^{(t)}$ The current hyperparameter vector at iteration t, η is the learning rate controlling adjustment speed. $\nabla Eval_{Score}(\theta)$ is the gradient or direction of improvement based on the evaluation score. These equations enable Evalmax Hyper Net to iteratively converge toward the best-performing hyperparameter configuration, balancing learning efficiency, generalization, and robustness across multiple validation folds.

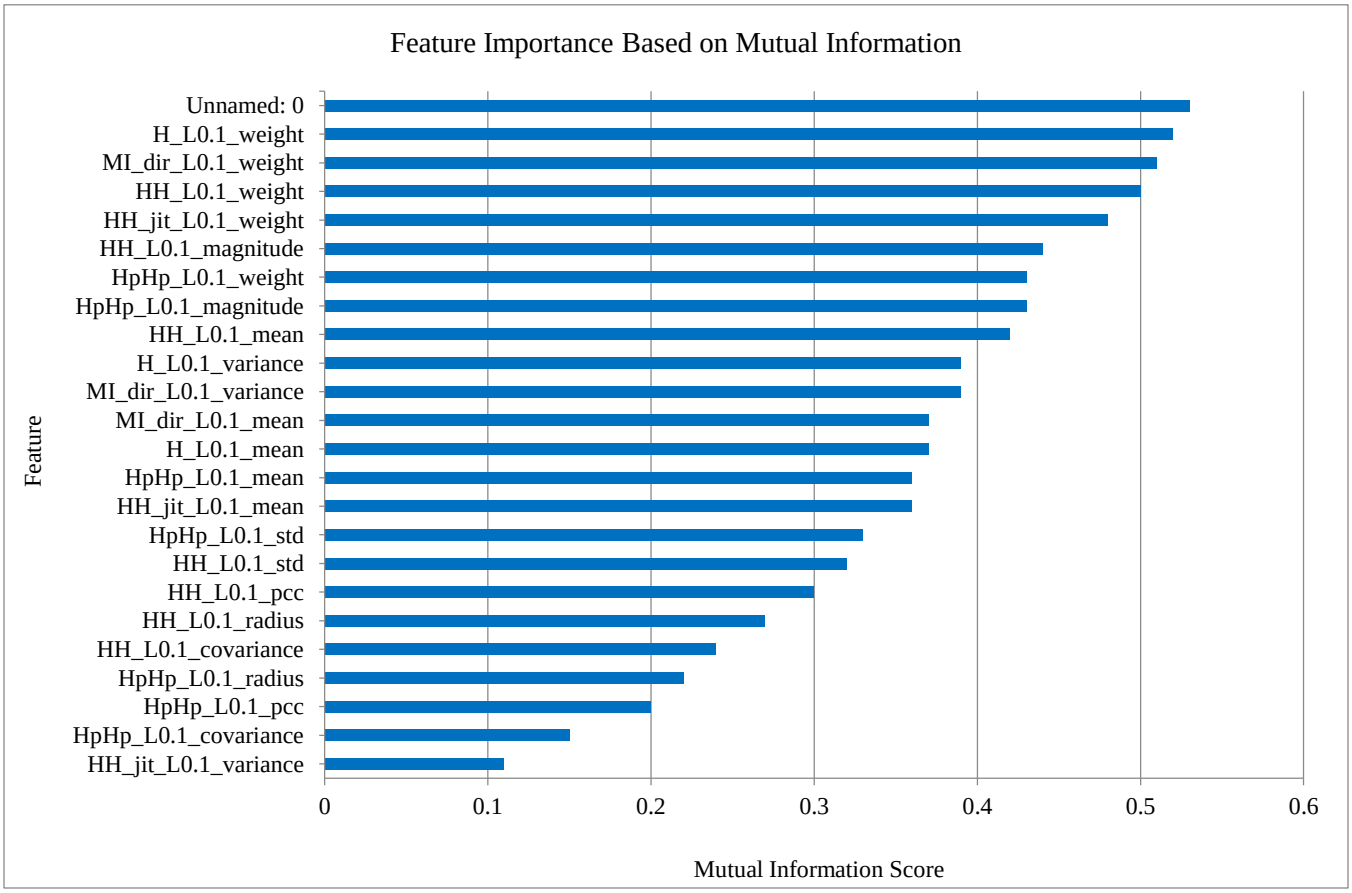

Fig. 2 Feature selection Output

4. Results and Discussion

This section outlines the experimental study conducted to evaluate the efficacy of the suggested intrusion detection in an IoT network.

4.1. Simulation Setup

The suggested research methodology is simulated using Python 3.9.6. This tool proves to be highly effective and meets all the required specifications outlined in the proposed methodology. The system specifications are detailed in Table 2.

Table 2. System configuration

Category	Specification
Operating System	Windows 10 (64-bit)
Development Platform	Anaconda with Jupyter Notebook
Python Environment	Version 3.9.6
Memory (RAM)	4 GB
Storage Capacity	500 GB Hard Drive

The bar chart showcases the feature importance scores based on mutual information, indicating how predictive each feature is for the target variable. Scores that are higher indicate features that are more informative, whereas lower scores indicate less informative features. Figure 2 shows the output of our feature selection.

4.2. Comparative Analysis

In this section, the effectiveness of the suggested method is assessed using performance metrics like "Accuracy, precision, F1-Score and Recall" and compared to numerous other approaches, including "Bald Eagle Search Optimization with Hybrid Deep Learning" (BESO-HDL) [18], Modified Isolation Forest (MIF) [19].

4.2.1. Accuracy

An accuracy is illustrated by how many of its predictions turn out to be accurate. Equation (12), the following is used to compute it:

$$H = \frac{\vartheta + R}{I + R + \sigma + N} \tag{12}$$

The number of cases that have been correctly identified and classified as such is represented by True Positive (ϑ). The number of correctly categorized as such is indicated by True Negative (R). The number that was mistakenly included as part of the data is represented by the false positive (σ) statistic. False negative (N) indicates the quantity of instances in Figure 3 and Table 3.

Table 3. Numerical outcomes of accuracy

No of Epochs (x-axis)	Accuracy (%)- (y-axis)		
	BESO-HDL	MIF	Proposed
20	0.65	0.75	0.85
40	0.67	0.77	0.87
60	0.66	0.76	0.89
80	0.72	0.82	0.9
100	0.75	0.85	0.95

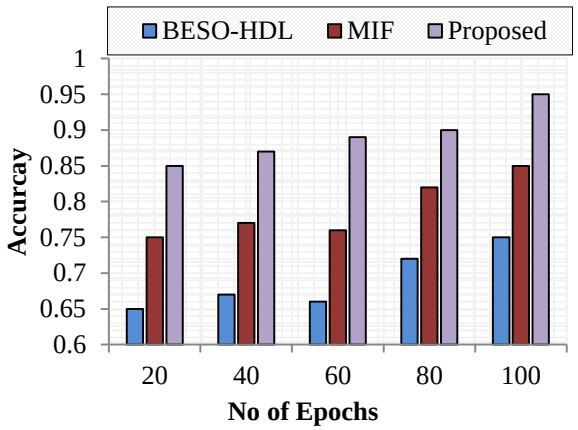

Fig. 3 Accuracy

4.2.2. Precision

The precision changes over time as the model trains, as shown by the Number of Epochs vs. Precision (%) graph. Out of all the positive predictions the model makes, precision (ρ) indicates the percentage of true positive predictions. An equation is used to calculate it.

$$\rho = \frac{\vartheta}{\vartheta + \sigma} \tag{13}$$

Where ϑ represents the true positives, σ indicates the false positives. This measure is essential for comprehending the model's accuracy in identifying positive cases while avoiding the error of misclassifying negative cases as positive in Figure 4 and Table 4.

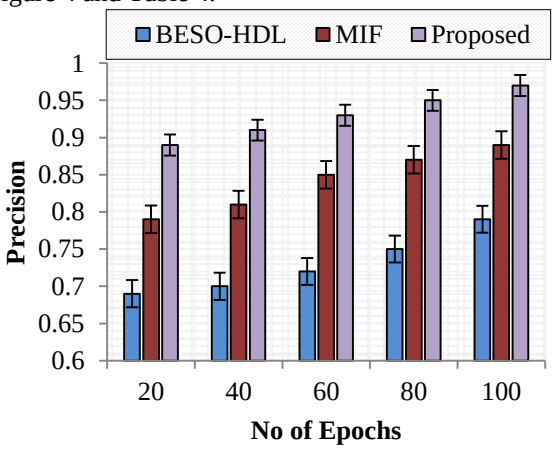

Fig. 4 Precision

Table 4. Numerical outcomes of precision

No of Epochs (x-axis)	Preccision (%)- (y-axis)		
	BESO-HDL	MIF	Proposed
20	0.69	0.79	0.89
40	0.7	0.81	0.91
60	0.72	0.85	0.93
80	0.75	0.87	0.95
100	0.79	0.89	0.97

4.2.3. Recall

The model's capacity to capture all positive occurrences over all epochs is finally gauged by the Number of Epochs vs. Recall (%) graph. Recall, which is the same as sensitivity, is computed as

$$\delta = \frac{\vartheta}{\vartheta + N} \tag{14}$$

It is a critical metric in situations where missing positive cases are especially harmful because it indicates how well the model detects all true positive cases. Recall monitoring aids in ensuring that the model's predictions are not overly conservative in Figure 5 and Table 4.

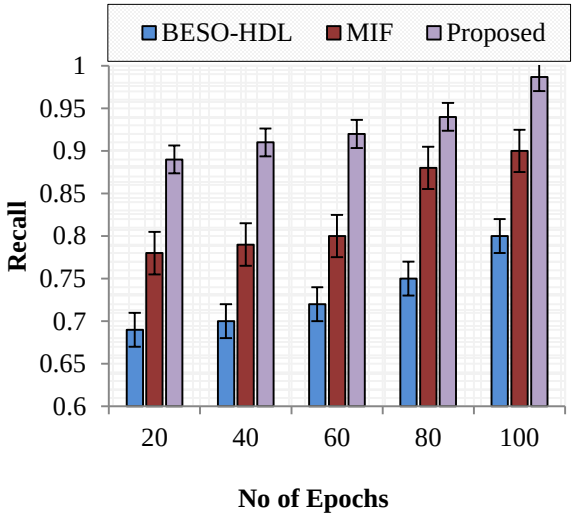

Fig. 5 Recall

Table 5. Numerical Outcomes of Recall

No of Epochs (x-axis)	Recall (%)- (y-axis)		
	BESO-HDL	MIF	Proposed
20	0.69	0.78	0.89
40	0.7	0.79	0.91
60	0.72	0.8	0.92
80	0.75	0.88	0.94
100	0.8	0.9	0.9867

4.2.4. F1- Score

The F-score is defined as the harmonic mean of recall and precision, respectively, with the product of two. Figure 6 and Table 6 demonstrate the f1-score. The formulation of the F-score can be provided as follows,

$$F - score = 2 \times \left(\frac{Prec \times Recc}{Prec + Recc}\right) \tag{15}$$

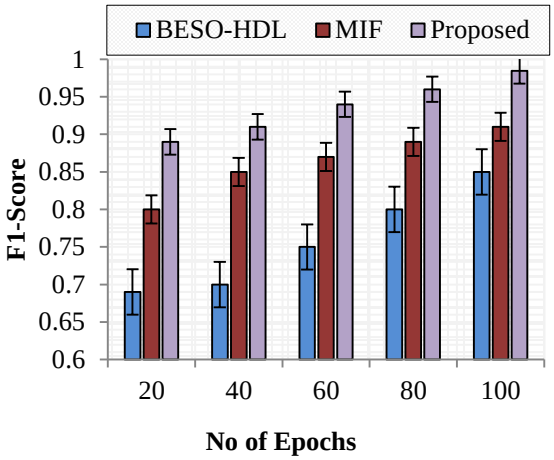

Fig. 6 F1-Score

Table 6. Numerical outcomes of F1-score

No of Epochs (x-axis)	F1-score (%)- (y-axis)		
	BESO-HDL	MIF	Proposed
20	0.69	0.8	0.89
40	0.7	0.85	0.91
60	0.75	0.87	0.94
80	0.8	0.89	0.96
100	0.85	0.91	0.9845

Here, Figure 8 indicates the confusion matrix, and they achieve the actual and predicted value of the proposed method. The output value of ROC and AUC is 0.9999. The confusion matrix shows the model correctly classified 39,401 normal instances and 9,933 attack instances. However, it misclassified 666 attacks as normal, indicating a small false negative rate. The ROC curve demonstrates the model's ability to differentiate among classes, with the curve hugging the top-left corner indicating high sensitivity and specificity. The Area Under the Curve (AUC) value of 0.9999 signifies exceptional model performance with almost perfect classification capability. This high AUC reflects a very low false positive rate and an excellent true positive rate in the model's predictions in Figure 7.

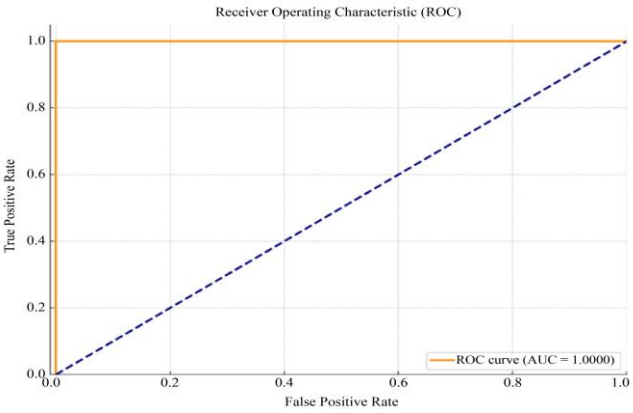

Fig. 7 AUC and ROC curve

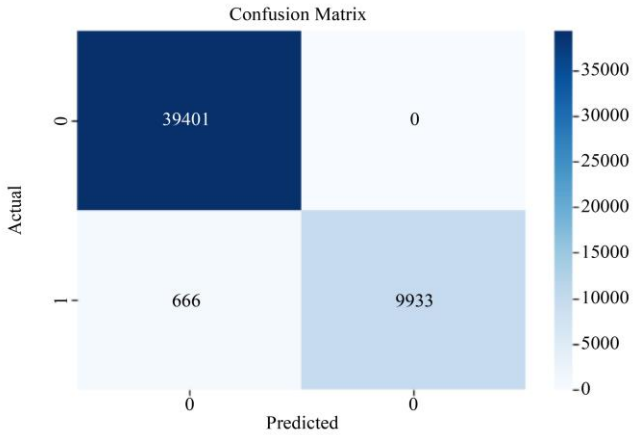

Fig. 8 Confusion matrix

The analysis of the carried out experiment shows that the given framework is significantly superior to the existing intrusion detection techniques in all main characteristics of its effective work. Accuracy values rise with each gain of training epoch, approaching 95 percent of accuracy at 100 epochs, a much higher rate than other solutions to the task of combating word embedding attacks, including BESO-HDL and Modified Isolation Forest. Equally, precision was improved to 97% showing that the model had a deficiency in detecting false positives. Recall was about 98.6 percent, which indicates the ability of the framework to show almost all instances of attacks. The F1-score that trades off between recall and precision scored 98.4, again indicating the soundness of the system. Other than this, the confusion matrix indicated that the model was able to correctly interpret most of the normal and attack instances without providing substantial false negative results. The ROC curve closely emerged along the top-left line with an AUC of 0.9999, which is close to a perfect classification ability.

The combination of the offered methods explains such results. The Cat-Scale normalization also avoided overrepresentation of mixed-type features, thereby speeding up the training process. Mutualk-Best feature selection alleviated redundancies and gave a compact yet informative feature set that was more efficient in classifier performance. Opto-Romar Swarm Bee Genesis model was indeed able to incorporate the best features of all three methods, PSO, ABC and GA to maintain a balance between exploration and exploitation, avoiding local minima and expediting convergence. Lastly, the Evalmax Hyper Net automatically tuned its hyperparameters using several evaluation metrics, contributing to a better possibility of generalization and stability regarding training epochs. Such synergy between preprocessing, feature selection, hybrid optimization, and adaptive tuning is why the proposed framework had an improved accuracy, recall, and robustness compared to state-of-the-art techniques.

Unlike the previous IDS models, which optimized one of the aforementioned steps only, the proposed model optimizes all of them in a single end-to-end pipeline that is specifically suited to the IoT scenario. The whole-thing design allows high accuracy and low computational complexity, which is a feasible approach to use in real-world systems in which the devices have limited resources.

5. Conclusion

To summarize, the presented hybrid metaheuristic-based IDS can be used to provide outstanding intrusion detection in IoT networks due to the combined features of Cat-Scale normalization, Mutualk-Best feature selection, and Opto-Romar Swarm Bee Genesis optimization, as well as evaluation based on the Evalmax Hyper Net. It is observed that the framework exhibits better results in all metrics than the state-of-the-art methods, and at 100 epochs, the accuracy is 95%, the precision is 97%, the recall is 98.6%, and the F1-score is 98.4. The ROC curve had an AUC of 0.9999, which shows that the model performed with near-perfect classification capability and false positive rates that were also too low. The above findings demonstrate the strength of the proposed solution in identifying known and unknown intrusion patterns and reducing misclassifications. The framework provides high classification performance and smoothens adaptability to the emerging patterns of the attack, ensuring the two key shortcomings in conventional IDS systems are avoided. The results conclude that swarm intelligence and a genetic algorithm-based solution are a proven, robust method to design IDS tools that can be scalable and future-proof in nature towards IoT. In the future, the model will be advanced into practical implementation for IoT setups and, more so, in low-compute and low-memory devices like sensors and embedded controllers. Future work will involve the addition of adversarial resilience to support advanced cyber-attacks, increased flexibility in zero-day resilience, and reducing the framework's overhead using lightweight versions to support edge computing and mobile IoT system usage.

References

[1] Shubhkirti Sharma, Vijay Kumar, and Kamlesh Dutta, "Multi-Objective Optimization Algorithms for Intrusion Detection in IoT Networks: A Systematic Review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 258-267, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tarek Gaber et al., "Industrial Internet of Things Intrusion Detection Method using Machine Learning and Optimization Techniques," *Wireless Communications and Mobile Computing*, vol. 2023, no. 1, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Amjad Rehman Khan, "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ajay Kumar et al., "Intrusion Detection and Prevention System for an IoT Environment," *Digital Communications and Networks*, vol. 8, no. 4, pp. 540-551, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ayoub Si-Ahmed, Mohammed Ali Al-Garadi, and Narhimene Boustia, "Survey of Machine Learning based Intrusion Detection Methods for Internet of Medical Things," *Applied Soft Computing*, vol. 140, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Inês Martins et al., "Host-Based IDS: A Review and Open Issues of an Anomaly Detection System in IoT," *Future Generation Computer Systems*, vol. 133, pp. 95-113, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Arash Heidari, and Mohammad Ali Jabraeil Jamali, "Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions," *Cluster Computing*, vol. 26, pp. 3753-3780, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Joseph Bamidele Awotunde, and Sanjay Misra, "Feature Extraction and Artificial Intelligence-Based Intrusion Detection Model for a Secure Internet of Things Networks," *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, pp. 21-44, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Rashmita Khilar et al., "Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yakub Kayode Saheed, and Sanjay Misra, "A Voting Gray Wolf Optimizer-Based Ensemble Learning Models for Intrusion Detection in the Internet of Things," *International Journal of Information Security*, vol. 23, pp. 1557-1581, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mousa'b Mohammad Shtayat et al., "An Improved Binary Spider Wasp Optimization Algorithm for Intrusion Detection for Industrial Internet of Things," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 2926-2944, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yakub Kayode Saheed et al., "A Novel Hybrid Autoencoder and Modified Particle Swarm Optimization Feature Selection for Intrusion Detection in the Internet of Things Network," *Frontiers in Computer Science*, vol. 5, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mohammed Aljebreen et al., "Enhancing DDoS Attack Detection using Snake Optimizer with Ensemble Learning on Internet of Things Environment," *IEEE Access*, vol. 11, pp. 104745-104753, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Abdullah Alzaqebah et al., "A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System," *Mathematics*, vol. 10, no. 6, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sandhya Ethala, and Annapurani Kumarappan, "A Hybrid Spider Monkey and Hierarchical Particle Swarm Optimization Approach for Intrusion Detection on Internet of Things," *Sensors*, vol. 22, no. 21, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Fahad F. Alruwaili et al., "Red Kite Optimization Algorithm with Average Ensemble Model for Intrusion Detection for Secure IoT," *IEEE Access*, vol. 11, pp. 131749-131758, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Khalid A. Alissa et al., "Planet Optimization with Deep Convolutional Neural Network for Lightweight Intrusion Detection in Resource-Constrained IoT Networks," *Applied Sciences*, vol. 12, no. 17, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Louai A. Maghrabi et al., "Enhancing Cybersecurity in the Internet of Things Environment using Bald Eagle Search Optimization with Hybrid Deep Learning," *IEEE Access*, vol. 12, pp. 8337-8345, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Orieb AbuAlghanam et al., "Fusion-Based Anomaly Detection System using Modified Isolation Forest for Internet of Things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 131-145, 2022. [CrossRef] [Google Scholar] [Publisher Link]