ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

Enhancing WSN Intrusion Detection: A Combined Deep Learning Framework with Dimensionality Reduction and Hybrid Optimization Technique

[1] Dilip Dalgade, [2] Nilesh Patil, [3] Manuj Joshi, [4] Dilendra Hiran

[1] Research Scholar, Department of Computer Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, India

[2] Co-Supervisor, Department of Computer Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, India

[3] Supervisor, Department of Computer Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, India

[3] Professor, Department of Computer Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, India

***Abstract*— Wireless Sensor Networks (WSNs) are susceptible to attacks as they are limited in resources and open in nature. Class-imbalance and high-dimensional data are likely to lead to poor performance of conventional intrusion detection systems (IDS). A hybrid solution to improving IDS performance in WSNs using deep learning, feature selection, and dimensionality reduction is presented in this paper. The model uses Principal Component Analysis (PCA) and Uniform Manifold Approximation and Projection (UMAP) as dimensionality reduction techniques, Particle Swarm Optimization (PSO) and Harris Hawks Optimization (HHO) as feature selectors, and Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) networks as classifiers. For handling class imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) is utilized on the NSL-KDD dataset for binary and multiclass labels.**

The performances show that the model proposed has accuracy metrics of 99.08% and 98.71% for binary and multiclass classification, respectively, which are higher compared to other methods. This hybrid technique effectively identifies different kinds of attacks, such as low-frequency R2L and U2R attacks, indicating the strength of advanced machine learning methods in intrusion detection within WSNs.

***Index Terms*— Wireless Sensor Networks, Intrusion Detection, UMAP, HHO-PSO, CNN- BiLSTM, Dimensionality Reduction, Feature Selection, SMOTE.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as advance technology that provides the ability for the collection, processing, and dissemination of data from sensor nodes distributed across a variety of locations. Sensor nodes typically contain various sensors and communication capabilities to monitor and low-level detect environmental situations. WSNs are used in military defence, industrial automation, and healthcare. This makes them susceptible to attacks as they are open and resource constrained. These factors enable remote data collection from hazardous areas for decision-making. These attacks risk data integrity, confidentiality, and availability, which affect organizations[1] [2].

Decision support systems in many fields rely on machine learning which is a growing field in computer science. In most cases, working with high-dimensional data is a big challenge to deal with. Traditional IDS techniques yield suboptimal results owing to high-dimensional characteristics and unbalanced class distributions [3] and often struggle to balance detection accuracy with resource efficiency, particularly when dealing with imbalanced datasets and infrequent attacks.

High-dimensional features and redundant data can reduce classifier performance, often leading to more false alarms. Many current solutions do not effectively address the need for clarity and precision in situations with different types of attacks. These issues call for a new method that deals with data imbalance, feature relevance, and time-related dependencies. This study presents a hybrid deep learning framework. It combines feature selection, dimensionality reduction, and temporal pattern modeling to enhance detection across various attack types on the NSL-KDD dataset by using both binary and multiclass labels as shown in figure 1.

The main contributions of the study are:

- In order to alleviate the class imbalance problem, we propose a concept of SMOTE, which improved detection ability of the minority class.
- A dimensionality reduction technique like UMAP and PCA to tackle the challenges of high-dimensional and noisy data and hybrid strategy metaheuristic feature selection methods such as HHO with PSO are utilized as wrapper-based approaches to iteratively pinpoint the most informative feature subsets for classification purposes in intrusion detection systems.
- The integration of Convolutional Neural Networks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

(CNNs) and Bidirectional Long Short-Term Memory (BiLSTM) networks allows for the effective capture of both spatial and temporal features from the optimized feature set.

The remainder of this paper is organized as follows. Section 2 reviews the research on intrusion detection, focusing on deep learning and other methodologies, and identifies their limitations. Section 3 details the proposed methods for dimensional reduction and feature selection, followed by experimental setup and data description in section 4. Experimental results showing the model's success in improving the IDS classification accuracy and comparative study in Section 5. Section 6 presents a summary of the study and outlines potential future developments for the system.

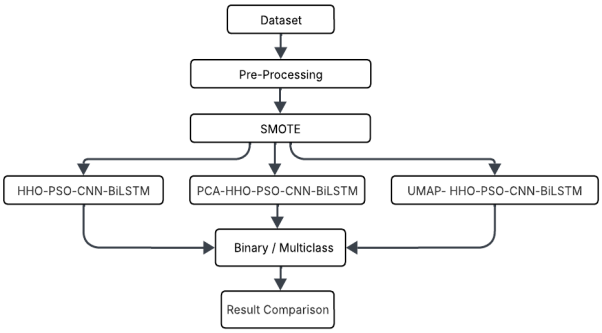


Fig. 1. Models compared in this research

II. RELATED WORK

In the field of intrusion detection, researchers have utilized various dimensional reduction, feature selection techniques, to derive a subset of features that can enhance the performance of these systems.

In [4]proposed a new model that combined a CNN with LSTM to improve intrusion detection. Furthermore, in [5]the developed LSTM-based models achieved impressive performance in recognizing various types of attacks by exploiting deep learning methods, such as PCA and Mutual Information, to minimize data dimensionality and extract features.

Several optimization-based deep learning models have also been introduced to improve IDS performance. In [6]introduced ILSTM, a new version of the Long Short-Term Memory (LSTM) algorithm. This helps detect network security threats more accurately. ILSTM uses the Chaotic Butterfly Optimization algorithm (CBOA) and Particle Swarm Optimization (PSO) to perform better than the traditional LSTM and other deep learning models in terms of accuracy and precision.

Similarly, Hybrid frameworks have been developed to address these emerging threats. In [7] introduced a defence mechanism based on the Harris Hawk optimization approach and "deep belief networks (DBN)" for WSNs to improve intrusion detection. In [8] proposed a new and efficient system, a hybrid framework that containing "Convolutional Neural Networks, Long Short-Term Memory Networks" and Extra Gradient Boosting to identify novel attacks. In [9]proposed HHO-MLP approaches the process of finding the optimal parameters, including weights and biases, to mitigate intrusion detection issues in network systems.

This approach was evaluated using various datasets. to improve detection capabilities and proposed a new hybrid Harris Hawk method. In [10]This algorithm uses a feature-selection mechanism to remove repeated features. The KNN and DDAE were applied to the original data to solve the imbalance. Another innovation came from [11] presenting an FL-based SCNN Bi-LSTM model for intrusion detection in WSNs with the intention of preserving the performance and privacy. This model employs Federated Learning (FL) to maintain data privacy while detecting intrusions. In [12] introduced a new technique, Genetic Sacrificial Whale Optimization (GSWO), which enhances IDS by selecting optimal features. The model was executed under the GSWO-CatBoost scenario. In [13]introduced an intrusion detection system (IDS) for wireless sensor networks (WSN) using particle swarm optimization (PSO) and ensemble machine learning. This approach combines RF, DT, and KNN models to improve detection accuracy. The system handles imbalanced datasets using LIME and SHAP.

III. PROPOSED METHODOLOGY

This section includes the data preprocessing, dimensionality reduction, feature selection, deep learning and proposed model implementation and parameters. The NSL-KDD dataset includes several types of attack labels and comes with a solid set of features, plus it mimics real traffic patterns. The training dataset contained 125,973 records, whereas the test dataset comprised 22,544 records. The training data, which included 41 features distributed into four primary groups of intrusion attack types: DoS, Probe, U2R, and R2L. The NSL-KDD dataset was of a sufficient size to facilitate its comprehensive practical application, yielding consistent and comparable results across various studies[2].

A. Data Preprocessing

The dataset was pre-processed to ensure its suitability for training and evaluation.

The preprocessing steps are as follows:

- To handle the missing data in the dataset, numeric features using the median, mode for categorical features.
- To address imbalanced data, SMOTE is applied to oversample the minority classes, ensuring a balanced distribution of classes in the training data.
- Binary classifications are mapped: normal = 0 and attack = 1.
- Multiclass are mapped: dos =0, normal = 1, probe = 2, r2l = 3, and u2r = 4.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

B. Dimensionality Reduction

UMAP and PCA are dimensionality reduction techniques utilized to reduce dimensionality and eliminate redundant features. These both algorithms managed to reduce redundancy by 26% by selecting 30 dimensions from the 41 features, which emphasizes that the features of the data structure were held within the data that can be retained.

UMAP is a nonlinear dimensionality reduction method based on manifold theory and fuzzy topology to project data in a high-dimensional space to a lower-dimensional space while maintaining local and global structures[14].

Fig.2 and Fig.3 show 2D UMAP projections for binary and multiclass data, respectively. The overlap among classes in multiclass projections indicates the challenge of discriminating between similar attacks.

The exponential probability distribution of high-dimensional points is used to calculate similarity:

$$p_{i|j=exp\left(-\frac{d(x_i,x_j)-\rho_i}{\sigma_i}\right)} \quad (1)$$

where $d(x_i, x_j)$, is the Euclidean distances between the points x_i and x_j. ρ_i is the distance to the nearest neighbor (used to control the density). σ_i is a local scaling factor that ensures uniformity across the different densities. The fuzzy simplicial set is then constructed by symmetrizing these probabilities:

$$p_{i|j} = p_{i|j} + p_{j|i} - p_{i|j} \cdot p_{j|i} \quad (2)$$

$$q_{\{ij\}} = \left(1 + a\,|\,y_i - y_j|^{\{2b\}}\right)^{\{-1\}} \quad (3)$$

Where $|\,y_i - y_j|$ is the squared Euclidean distance in a low-dimensional space [15].

Principal component analysis (PCA) is a technique for reducing dimensionality by creating new, uncorrelated variables that progressively increase variance and aids in minimizing errors during parameter estimation and reduces the computational cost by either minimizing the dimensions in the attribute space or identifying a subspace that most effectively represents the core of the data[5]. Fig. 4 shows the explained variance for each principal component. Normalization factor to ensure an unbiased estimate of covariance.

$$C_{v_{jk}} = \left(\frac{1}{n-1}\right)\sum_{i=1}^{n}(x_{ij} - x'_j)(x_{ik} - x'_k)] \quad (4)$$

This equation computes the covariance between two features j and k.

$(x_{ij} - x'_j)(x_{ik} - x'_k)$,' the product of the deviations from the mean, measures the extent to which the two features vary.

Use of dimension reduction techniques such as PCA or UMAP can help reduce extraneous information and convert complex high dimension data into something more manageable. Not only does this method simplify the computational task, it also reveals the most critical patterns in the data. By focusing on such a reduced set of dimensions, the later feature selection should have greater likelihood of being able to find the most important features, and thus the effort of optimization will be directed at informative features and not at arbitrary noise.

C. Hybrid Feature Optimization

The hybrid HHO-PSO optimization method is used to find the best feature subset from a reduced feature space. This method combines the exploration strengths of Harris Hawks Optimization (HHO) with the refinement capabilities of Particle Swarm Optimization (PSO) as illustrated in Figure 2.

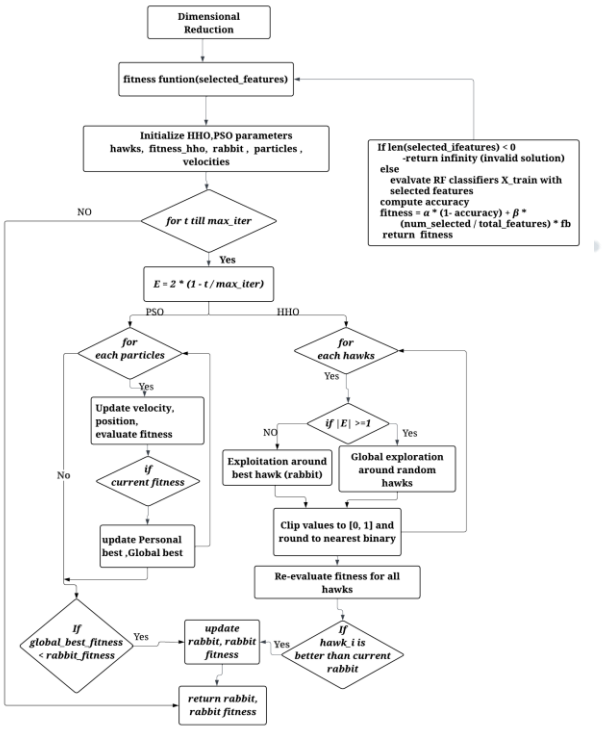


Fig. 2. Flowchart of hybrid optimization method

a. Construction of Feasible Solutions

The initial populations of hawks (HHO agents) and particles (PSO agents) are randomly generated binary vectors $F \in \{0,1\}^{\{d\}}$, where d is the number of projected features. Each agent represents a feature selection mask.

The fitness of each agent is calculated to balance two objectives: classification performance and the compactness of the feature subset.

$$F = \alpha \cdot (1 - Accuracy) + \beta \cdot \left(\frac{SL}{FN}\right) \times fb \quad (5)$$

A *Random Forest* classifier evaluates accuracy for the selected subset. Were, *F* denotes fitness, which is likely to be as low as possible, α is the classification error weight, and β is the feature-selection penalty weight. *Accuracy* is the classification accuracy, *SL* is the selected feature count, and *FN* is the total number of features. The *fb* factor balances the feature selection with accuracy.

b. Harris Hawk Optimization: (Exploration–Exploitation Strategy)

The hawks represent candidate feature subsets, and their

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

positions are updated using exploration or exploitation strategies based on the energy level [7][10][16].

HHO uses *escape energy* $E = 2E_0\left(1 - \frac{t}{T}\right)$, which controls the transition from exploration

(|E| ≥ 1) to exploitation (|E| < 1). where E is the cost of evaluating the fitness (i.e., training and validating a classifier).

If |E|≥1, hawks perform exploration using:

$$S_i^{\{(t+1)\}} = S_{rand} - r \cdot | S_{rand} - 2r \cdot S_i^{\{(t)\}} | \quad (6)$$

If |E|<1, hawks perform exploitation, imitating a hard besiege strategy:

$$S_i^{\{(t+1)\}} = S_{rabbit} - E \cdot | S_{rabbit} - S_i^{\{(t)\}} | \quad (7)$$

All updates are binarized using thresholding (0.5) to retain valid binary feature masks.

Here: S_{rand}: random hawk solution, S_{rabbit}: best solution so far (global best),

r: random number ∈[0,1]

c. Particle Swarm Optimization: (Swarm Fine-Tuning)

PSO simulates the social behavior of bird flocks to solve optimization problems. The particles traverse the solution space and update their velocities using both local and global bests [13]. PSO fine-tunes the candidate solutions by updating particle velocities and positions based on both individual and collective experiences. At each iteration *t*, the velocity of particle *i* is updated according to:

$$v_i^{t+1} = \omega v_i^t + c_1 r_1 (p_i - x_i^t) + c_2 r_2 (g - x_i^t) \quad (8)$$

Where v_i^t is the velocity at iteration *t*, p_i is the personal best, *g* is the global best, ω is the inertia weight, and *c1*,*c2* are cognitive and social learning factors.

The optimization process happens in two stages: first, HHO performs global exploration. Then, PSO fine-tunes the best solutions to improve both accuracy and compactness. A Random Forest classifier assesses the feature masks, and the mask with the lowest fitness score is selected as the final feature subset. Figure 3 shows the hyperparameters used in the HHO-PSO algorithm to select the number of features for classification.

Parameter	Description	Value
hawks	Number of search agents in HHO. Each hawk represents a candidate feature subset.	20
alpha	Exploration vs. exploitation trade-off in HHO.	0.80
particles	Number of candidate solutions (particles) in PSO.	20
beta	Velocity adjustment factor in PSO.	0.2
max_iter	Number of iterations for HHO-PSO to refine feature selection.	5

Fig. 3. Parameters used in HHO-PSO Feature Selection

D. Hybrid CNN + BiLSTM Model

To finalize classification, we integrated a Convolutional Neural Network (CNN) with a Bidirectional Long Short-Term Memory (BiLSTM) network prediction model as shown in figure 4. CNN extracts spatial features from the input feature vector using convolutional layers.

BiLSTM captures temporal dependencies in both the forward and backward directions, which is crucial for identifying attack patterns that may occur in sequences. The hybrid model improved the performance for intrusion detection in wireless sensor networks (WSNs). The parameters used to configure the CNN-BiLSTM architecture are listed in figure 5.

IV. EXPERIMENTAL SETUP AND DATA DESCRIPTION

A. Experimental Setup

The model was developed using the Jupyter Notebook with Python 3.11, using the Scikit-learn, Seaborn, Matplotlib, NumPy, Keras, and Pandas libraries. The computing environment ran on Windows 11 Professional and used a 500GB SSD, 16GB RAM, and an Intel Core i7-8665U CPU running at 1.90GHz (two cores and four logical processors).

B. Data Description

The NSL-KDD dataset was segmented in a Jupyter notebook setting into a 20% testing set, while 80% of the training set maintained the class distribution. SMOTE is an oversampling method that balances the training data classes. The NSL-KDD dataset has 41 features, three of which are categorical: protocol_type, service, and flag. One-hot encoding was used to make sure these features would work with learning models. This process brings the 41-dimensional features to total 122 after encoding. While this increase preserves categorical semantics creates a higher computational burden. To improve efficiency, reduce overfitting and scalability, dimensionality reduction was used before metaheuristic feature selection.

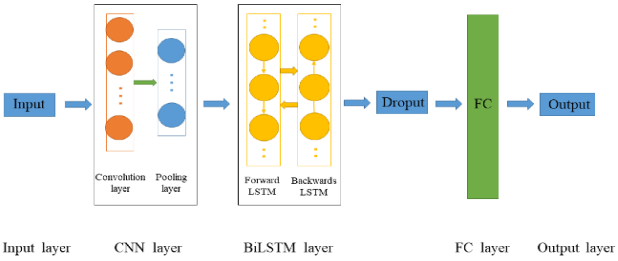


Fig. 4. Structure of CNN-BiLSTM [17].

Parameter	Binary Classification	Multiclass Classification
Loss Function	Huber Loss	Categorical Crossentropy
Conv1D	Filters: 32,64 Kernel Size: 2, Activation: ReLU, Regularization: L2 (0.001)	Filters: 64, Kernel Size: 3, Activation: ReLU, Regularization: L2 (0.001)
MaxPooling1D	Pool Size: 2	Pool Size: **2**
Bidirectional LSTM	Layer 1: Units: 64, Return Sequences: True, Regularization: L2 (0.001) Layer 2: Units: 32, Return Sequences: False, Regularization: L2 (0.001)	Layer 1: Units: 128, Return Sequences: True, Regularization: L2 (0.001) Layer 2: Units: 64, Return Sequences: False, Regularization: L2 (0.001)
Epsilon	1e-08	1e-08
Optimizer	Adam	Adam
Learning Rate	0.002	0.002
Epochs	50	50
Dropout	0.2	0.2
Activation	Sigmoid	Softmax

Fig. 5. CNN–BiLSTM Configuration Parameters.

V. RESULT ANALYSIS AND DISCUSSION

A. Experimental results

In this study, the results obtained from binary and multi-class classification with five categories were used. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

performance of each model was determined using the accuracy, precision, recall, F1-score, FPR, FNR, FDR of the evaluation matrix obtained based on the parameters TP, TN, FN, FP which are used to measure the actual performance of the model. Table 1 and Table 2 presents the performance of several feature optimization and dimensionality reduction techniques applied to the binary and multiclass classification task. Additionally, the number of selected features for each approach is reported. PCA-HHO+PSO achieves the highest performance across all metrics, with an accuracy of 99.08%, FPR of 0.0088 and accuracy of 98.71%, FPR of 0.0031 in binary and multiclass classification respectively. Figure 7 presents the confusion matrix for binary and multiclass classification.

To evaluate multiclass classification on the NSL-KDD dataset, ROC curves were plotted for each class across UMAP–HHO+PSO–CNN+BiLSTM and PSO–HHO+PSO–CNN+BiLSTM configurations (Figure 8). The curves represent dos, normal, probe, r2l, and u2r classes, with AUC scores indicating model performance. In the UMAP configuration, the model achieved perfect classification (AUC = 1.00) for dos, normal, probe, and r2l classes, but performed poorly for u2r (AUC = 0.98). The PSO configuration maintained high AUC scores for major classes while improving u2r detection (AUC = 1.00), suggesting PSO-first feature selection provides more discriminative features before hybrid optimization and deep learning stages. This confirms PSO's advantage as an initial feature selector and shows that strategic ordering of selection techniques significantly impacts classification effectiveness in intrusion detection systems. Figure 9 illustrate the classification report for the multiclass classification for UMAP and PCA.

B. Error Rate Comparison

Figure 10 compares False Positive Rate (FPR), False Negative Rate (FNR), and False Discovery Rate (FDR) across six models for binary and multiclass classification on NSL-KDD dataset. UMAP–HHO+PSO and PCA–HHO+PSO models show lowest error rates, indicating better detection reliability. PSO demonstrates lower FNR and FDR than ACO and HHO+PSO. HHO+PSO's high FNR and FDR values show hybrid optimization's sensitivity to feature representation. Dimensionality reduction through UMAP and PCA with hybrid optimization reduces false alarms and missed detections, highlighting the importance of feature selection with dimensionality reduction for improved model performance.

C. Discussion

These results were compared with those of previous studies to enhance our understanding of the experimental findings (Table 3). This comparison of various algorithms serves as a reference point. These findings indicate that different intrusion-detection systems can yield significantly varied results, complicating

the development of a universally optimal model. Our proposed models, UMAP-HHO+PCA-CNN+BiLSTM and PCA-HHO+PCO-CNN+BiLSTM, demonstrate superior performance compared to current leading methods in both binary and multiclass classification tasks. The PCA-HHO+PCO-CNN+BiLSTM model achieves the highest accuracy rates (99.08% for binary and 98.71% for multiclass), along with top precision, recall, and F1-score, outperforming models like [18], [6], [10], and the [7] hybrid. Although DBN-HHO and DNN exhibit strong binary classification capabilities, our models provide better results with balanced precision-recall and enhanced F1-scores. This advancement is due to the integration of feature optimization (HHO+PSO) and dimensionality reduction techniques (PCA, UMAP), which boost performance while minimizing feature dimensionality for more efficient models.

Dimensional Reduction using UMAP and PCA effectively reduced redundant features by more than 26% without sacrificing model accuracy (over 95% accuracy achieved). HHO+PSO could optimize the selection process of features out of a potential of 30 from the selected UMAP and PCA. The detection of infrequent attacks, such as R2L and U2R, was improved by applying SMOTE to the imbalanced datasets. The CNN's recall for DoS and Probe attacks is owing to its proficiency in capturing spatial relationships.

VI. CONCLUSION AND FUTURE WORK

The paper proposes an innovative hybrid model based on deep learning, feature selection, and dimensionality reduction to improve intrusion detection in Wireless Sensor Networks (WSNs). The model is accompanied by a deep learning classifier constructed using Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) networks.

The hybrid feature selection method that employs Harris Hawks Optimization (HHO) and Particle Swarm Optimization (PSO), along with Uniform Manifold Approximation and Projection (UMAP) and Principal Component Analysis (PCA) for dimensionality reduction.

Key findings are:

1. The dimensionality reduction methods (UMAP and PCA) were successful in reducing the duplicate features by 26% without compromising the model performance.
2. The hybrid HHO-PSO feature selection method enhanced the selection of informative features.
3. The combination of CNN-BiLSTM enhanced the detection of frequent as well as rare attacks such as DoS, Probe, R2L, and U2R.
4. The proposed model worked better in terms of precision, accuracy, recall, and F1-score with respect to the current methods.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

Table 3: Bianry classification comparative analysis of various feature optimization techniques (%).

	ACO (All Features)	PSO (All Features)	HHO (All Features)	HHO+PSO (All Features)	UMAP-HHO+PSO (30 component)	PCA-HHO+PSO (30 component)
Seleted Features	4	59	62	54	22	25
Accuracy	86.41	98.23	98.40	96.51	98.46	**99.08**
Precision	93.70	97.95	98.64	97.97	98.67	**99.12**
Recall	76.92	98.38	98.02	94.70	98.13	**98.97**
F1 score	84.48	98.16	98.33	96.31	98.40	**99.05**
FPR	0.0480	0.0125	0.0177	0.0182	0.0187	**0.0088**

Table 4: Multiclass classification comparative analysis various feature optimization techniques (%).

	ACO-(All Features)	PSO (All Features)	HHO All Features)	HHO+PSO (All Features)	UMAP-HHO+PSO (30 component)	PCA-HHO+PSO (30 component)
Seleted Features	2	46	74	16	17	12
Accuracy	73.40	98.07	98.01	79.82	97.37	**98.71**
Precision	48.51	89.71	90.45	54.24	80.25	**90.16**
Recall	56.94	92.90	90.98	78.42	86.52	**94.13**
F1 score	48.81	90.31	89.51	56.42	82.70	**91.88**
FPR	0.0662	0.0046	0.0048	0.0411	0.0064	**0.0031**

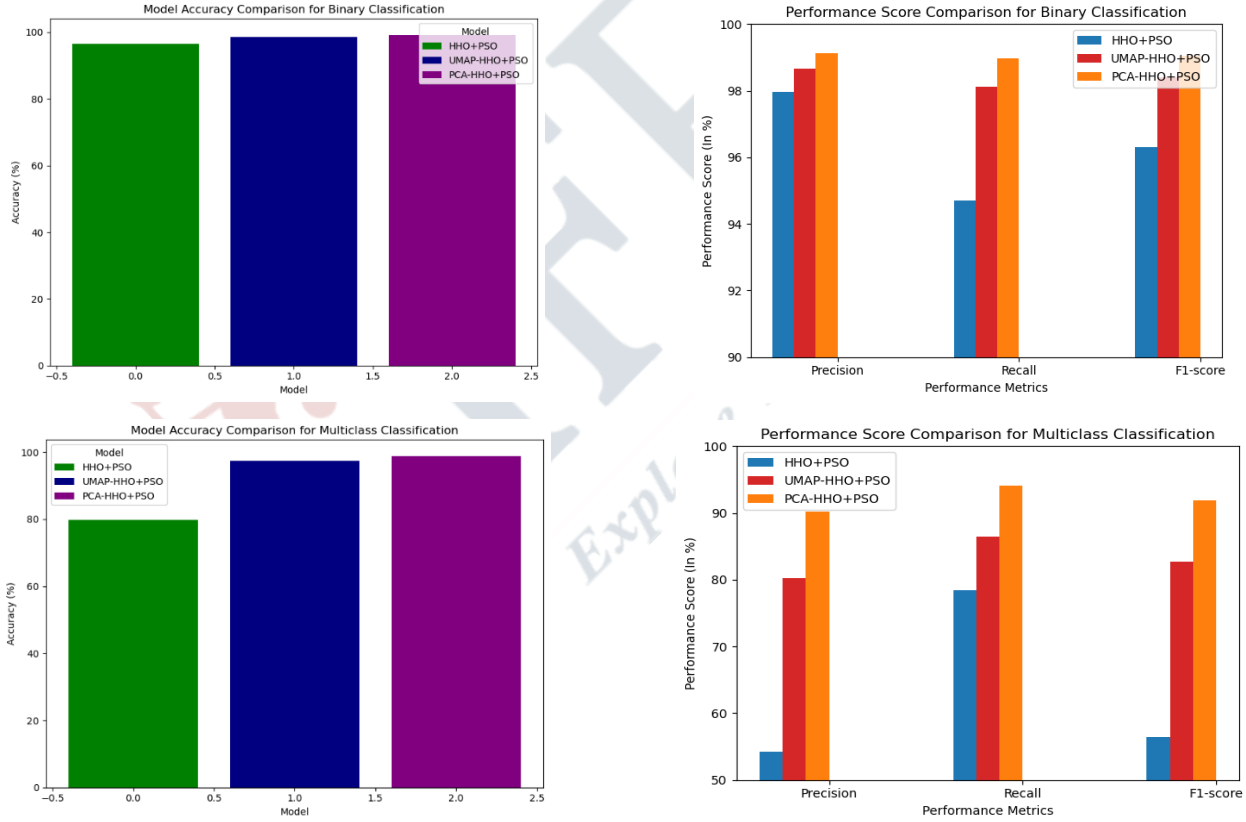


Fig. 6. Performance score comparison for Binary and Multiclass classification.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 09 September 2025

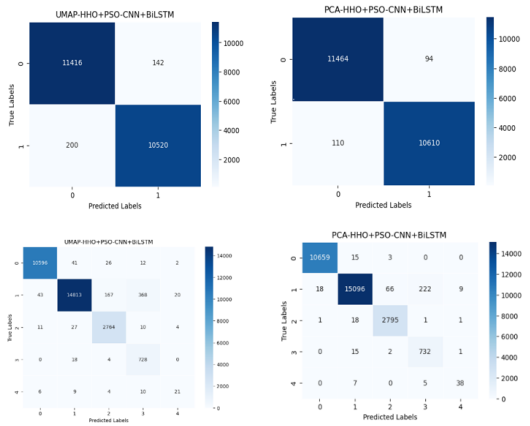


Fig. 7. Binary and Multiclass classification confusion matrix.

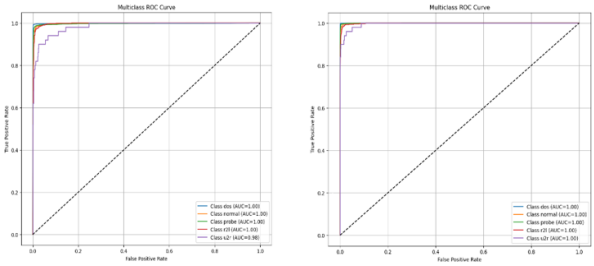


Fig. 8. ROC Curve of UMAP-HHO+PSO-CNN-BiLSTM and PSO HHO+PSO-CNN-BiLSTM Multiclass classification

Classification Reportof UMAP-HHO+PSO-CNN+BiLSTM:

	precision	recall	f1-score	support
dos	0.99	0.99	0.99	10677
normal	0.99	0.96	0.98	15411
probe	0.93	0.98	0.96	2816
r2l	0.65	0.97	0.78	750
u2r	0.45	0.42	0.43	50
accuracy			0.97	29704
macro avg	0.80	0.87	0.83	29704
weighted avg	0.98	0.97	0.97	29704

Overall F1 Metrics:
Macro-F1 : 0.8270
Micro-F1 : 0.9737
Weighted-F1 : 0.9750

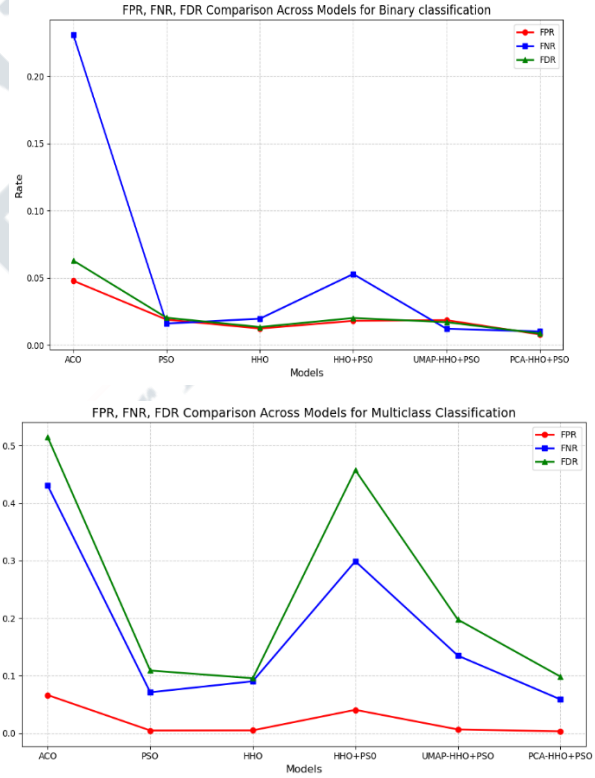
Classification Reportof PCA-HHO+PSO-CNN+BiLSTM:

	precision	recall	f1-score	support
dos	1.00	1.00	1.00	10677
normal	1.00	0.98	0.99	15411
probe	0.98	0.99	0.98	2816
r2l	0.76	0.98	0.86	750
u2r	0.78	0.76	0.77	50
accuracy			0.99	29704
macro avg	0.90	0.94	0.92	29704
weighted avg	0.99	0.99	0.99	29704

Overall F1 Metrics:
Macro-F1 : 0.9188
Micro-F1 : 0.9871
Weighted-F1 : 0.9875

(a) UMAP-HHO+PCA-CNN+BiLSTM (b) PCA-HHO+PSO-CNN+BiLSTM

Fig. 9. Classification Report for Binary and Multiclass Classication



(a) Binary classification (b) Multiclass Classification

Fig. 10. Compares FPR, FNR, and FDR Across Six Models.

Table 5: Comparative study

Study	Model	Accuracy		Precision		Recall		F1-Score	
		Binary	MC	Binary	MC	Binary	MC	Binary	MC
[18]	CNN-LSTM-SA	89.38	93.72	87.12	91.84	95.63	**95.02**	91.17	93.26
[6]	ILSTM	91.31	93.09	94.76	**95.86**	84.93	88.88	89.36	91.72
[10]	DNN	93.31	86.79	92.88	89.46	-	-	94.21	87.56
[7]	DBN-HHO	98.5		97.9		97.6		98.3	

Study	Model	Accuracy		Precision		Recall		F1-Score	
		Binary	MC	Binary	MC	Binary	MC	Binary	MC
Our Model	UMAP-HHO+PCA-CNN+BiLSTM	98.46	97.37	98.67	80.25	98.13	86.52	98.40	82.70
	PCA-HHO+PCO-CNN+BiLSTM	**99.08**	**98.71**	**99.12**	90.16	**98.97**	94.13	**99.05**	**91.88**

The findings forecast the potential that the usage of state-of-the-art machine learning methods holds to develop strong and efficient Intrusion Detection Systems for WSNs. The research findings supplement the current effort to improve security in environments that are constrained with resources.

Future enhancements of this framework can be explored in several directions, such as 1. Implement a framework for real-time intrusion detection on energy-limited sensor nodes using model compression and lightweight deep-learning models. 2. Adaptive feature selection mechanisms change feature subsets depending on the network conditions or features of attacks. 3. This needs to be examined using a variety of datasets (such as UNSW-NB15 and CICIDS2017) to ensure that its features are stable and move in various network contexts.

Author contributions: All the authors contributed equally to, read, and approved the final manuscript.

Funding: No funding.

Data Access Statement: Data is available based on the request.

Conflict of Interest: None of the authors have any conflict of interests to disclose

REFERENCES

[1] Md. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, "MLSTL-WSN: Machine Learning-based Intrusion Detection using SMOTETomek in WSNs," Feb. 2024, [Online]. Available: http://arxiv.org/abs/2402.13277

[2] G. M. Borkar, L. H. Patil, D. Dalgade, and A. Hutke, "A 01novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept," *Sustainable Computing: Informatics and Systems*, vol. 23, pp. 120–135, Sep. 2019, doi: 10.1016/j.suscom.2019.06.002.

[3] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning," *IEEE Access*, vol. 9, pp. 7550–7563, 2021, doi: 10.1109/ACCESS.2020.3048198.

[4] M. Ahsan and K. E. Nygard, "Convolutional Neural Networks with LSTM for Intrusion Detection."

[5] F. E. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *J Big Data*, vol. 8, no.1, Dec. 2021, doi: 10.1186/s40537-021-00448-4.

[6] A. A. Awad, A. F. Ali, and T. Gaber, "An improved long short term memory network for intrusion detection," *PLoS One*, vol. 18, no. 8 August, Aug. 2023, doi: 10.1371/journal.pone.0284795.

[7] Vikas, R. P. Daund, D. Kumar, P. Charan, R. S. K. Ingilela, and R. Rastogi, "Intrusion Detection in Wireless Sensor Networks using Hybrid Deep Belief Networks and Harris Hawks Optimizer," in *2023 4th International Conference on Electronics and Sustainable Communication Systems, ICESC 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1631–1636. doi: 10.1109/ICESC57686.2023.10193270.

[8] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *Journal of Cloud Computing*, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-024-00685-x.

[9] M. Alazab, R. A. Khurma, P. A. Castillo, B. Abu-Salih, A. Mart´ın, and D. Camacho, "An Effective Networks Intrusion Detection Approach Based on Hybrid Harris Hawks and Multi-Layer Perceptron."

[10] P. Zhou, H. Zhang, and W. Liang, "Research on hybrid intrusion detection based on improved Harris Hawk optimization algorithm," *Conn Sci*, vol. 35, no. 1, 2023, doi: 10.1080/09540091.2023.2195595.

[11] S. M. S. Bukhari *et al.*, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," *Ad Hoc Networks*, vol. 155, Mar. 2024, doi: 10.1016/j.adhoc.2024.103407.

[12] T. M. Nguyen, H. H. P. Vo, and M. Yoo, "Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach," *Sensors*, vol. 24, no. 11, Jun. 2024, doi: 10.3390/s24113339.

[13] S. A. Birahim *et al.*, "Intrusion Detection for Wireless Sensor Network using Particle Swarm Optimization based Explainable Ensemble Machine Learning Approach," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3528341.

[14] L. McInnes, J. Healy, and J. Melville, "UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction," Feb. 2018, [Online]. Available: http://arxiv.org/abs/1802.03426

[15] M. Allaoui, M. L. Kherfi, and A. Cheriet, "Considerably improving clustering algorithms using umap dimensionality reduction technique: A comparative study," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*,

Springer, 2020, pp. 317–325. doi: 10.1007/978-3-030-51935-3_34.

[16] T. Thaher, M. Saheb, H. Turabieh, and H. Chantar, "Intelligent detection of false information in arabic tweets utilizing hybrid harris hhawks-basedfeature selection and machine learning models," *Symmetry (Basel)*, vol. 13, no. 4, Apr. 2021, doi: 10.3390/sym13040556.

[17] Y. Su, H. Gan, and Z. Ji, "Research on Multi-Parameter Fault Early Warning for Marine Diesel Engine Based on PCA-CNN-BiLSTM," *J Mar Sci Eng*, vol. 12, no. 6, Jun. 2024, doi: 10.3390/jmse12060965.

[18] B. Hui and K. L. Chiew, "An Improved Network Intrusion Detection Method Based On CNN-LSTM-SA," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 44, no. 1, pp. 225–238, Feb. 2025, doi: 10.37934/araset.44.1.225238.