PENINSULA PUBLISHING LLC

EDRAAK
Vol. **(2026)**, 2026, **pp**. 52–74
ISSN: 3078-8412

Research Article

Modelling-Based Classification of Sensor Nodes in WBAN Using a Hybrid Backpropagated Mask Convolutional Neural Network

Israa Ibraheem Al Barazanchi [1, 2, *], Wahidah Hashim [1,], Reema Thabit [3,], Abdul Samad Bin Shibghatullah [4]

[1] *College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), 43000 Kajang, Selangor, Malaysia*
[2] *College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq*
[3] *School of Computer Science and Engineering, Taylor's University, Selangor 47500, Malaysia*
[4] *College of Computing & Informatics (CCI); Universiti Tenaga Nasional, Kajang, Selangor, Malaysia*

ARTICLE INFO

Article History
Received 12 Feb 2026
Revised: 26 Mar 2026
Accepted 25 Apr 2026
Published 10 May 2026

Keywords
WBAN,
Trust Node Classification,
Dragonfly optimization algorithm,
HB-MCNN,
Feature Selection,
Convergence Analysis.

ABSTRACT

Wireless Body Area Networks (WBANs) have enhanced cornerstone technology in modern healthcare, enabling continuous monitoring of patients through interconnected wearable sensors. However, their reliability and security remain vulnerable due to untrusted or malicious sensor nodes that can degrade data quality and delay medical responses. This study introduces an integrated intelligent framework that enhances node trust classification indoors healthcare-oriented WBAN environments. The proposed approach combines Principal Component Analysis (PCA) for dimensionality reduction with the Dragonfly optimization algorithm algorithm for optimal feature selection, followed by a Hybrid Backpropagated Mask Convolutional Neural Network (HB-MCNN) for node trust classification. The model was evaluated using a real WBAN dataset under controlled simulation settings. Results demonstrated a classification rate of 99.2%, an accuracy of 98.5%, a packet delivery rate of 98.6%, and a latency of 7.2 ms, while reducing energy consumption to 55.5%. These outcomes confirm the framework's ability to enhance the reliability and security of medical data transmission by accurately isolating untrusted nodes, reducing communication delays, and improving overall trust management in healthcare monitoring systems.

1. INTRODUCTION

Wireless Body Area Networks (WBANs) have emerged as a core component in next-generation healthcare systems, enabling continuous monitoring of physiological parameters through wearable and implantable sensors [1,2]. These intelligent systems enhance patient care by transmitting real-time biomedical information to medical servers, thereby facilitating timely diagnosis and treatment [3,4]. However, as WBANs operate through wireless communication between numerous sensor nodes, maintaining data confidentiality, integrity, and availability is essential to ensure secure and dependable healthcare services [5,6]. Recent studies have shown that the reliability of WBANs heavily depends on the trustworthiness of their sensor nodes [7]. Malicious or untrusted nodes may inject false readings, disrupt routing paths, or launch attacks such as selective forwarding and sinkhole intrusions, leading to inaccurate medical decisions and reduced system reliability [8,9]. Furthermore, the limited resources of WBAN nodes particularly energy, processing power, and memory make traditional cryptographic and trust management approaches unsuitable for continuous medical monitoring [10,11]. Trust-based classification has therefore become a key mechanism to identify and isolate untrusted nodes in WBAN environments. Several techniques have been proposed, including optimization algorithms and deep learning architectures, to enhance classification accuracy and reduce latency [12,13]. Figure 1 illustrates the Integrated Telehealth Monitoring Network with Wearable Sensors.

*Corresponding author email: israa.albarazanchi2023@gmail.com
DOI: https://doi.org/10.70470/EDRAAK/2026/005

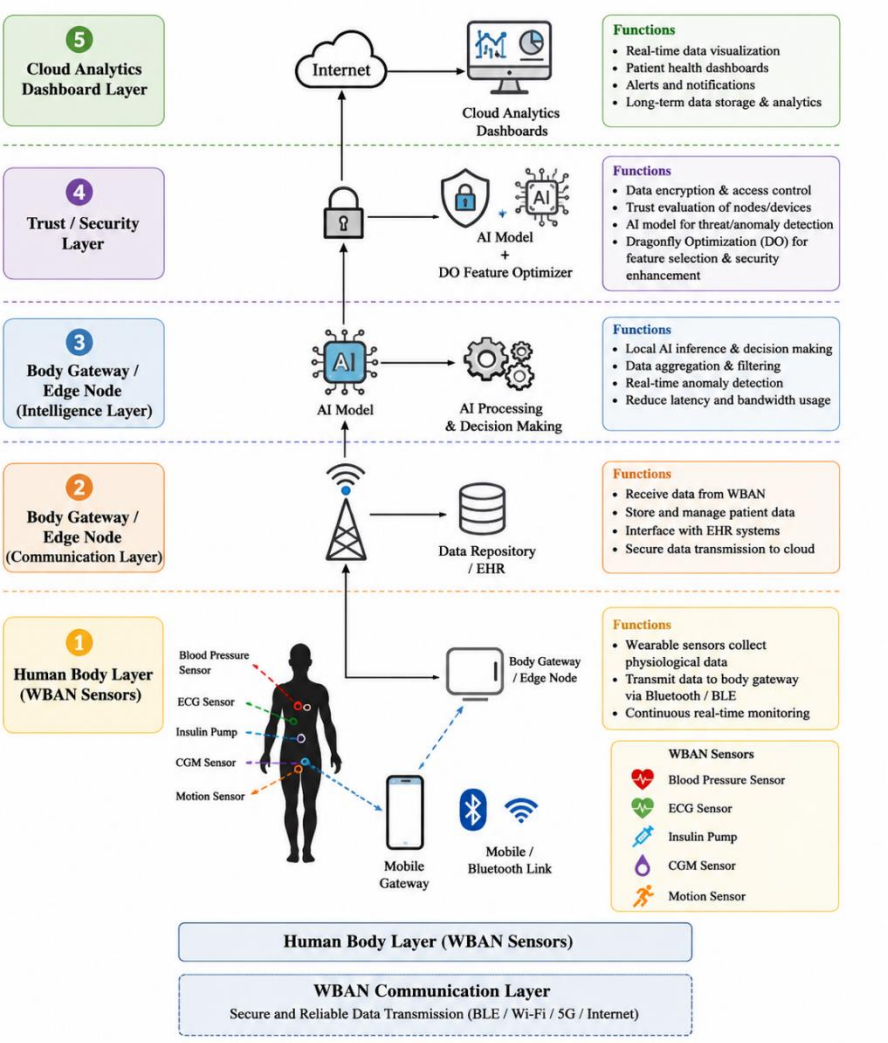


Fig. 1. Integrated Telehealth Monitoring Network with Wearable Sensors

Nevertheless, existing methods often suffer from slow convergence, high energy consumption, or insufficient adaptability to dynamic network conditions [14,15]. Moreover, many approaches focus exclusively on improving performance metrics such as latency or throughput without addressing the security implications of untrusted node behavior [16].

To address these challenges, this study proposes an integrated hybrid model that combines Principal Component Analysis (PCA) for dimensionality reduction, Dragonfly optimization algorithm (DO) for feature selection, and a Hybrid Backpropagated Mask Convolutional Neural Network (HB-MCNN) for node trust classification [17,18]. This combination allows the system to efficiently filter untrusted nodes, enhance classification precision, and minimize latency and energy consumption simultaneously. The model aims to establish a more secure, reliable, and resource-efficient framework for real-time health data transmission in WBAN-based healthcare applications.

2. RELATED WORK

Trust and security management in Wireless Body Area Networks (WBANs) has been extensively investigated due to the critical importance of sensor nodes in ensuring reliable healthcare data transmission. Several approaches have focused on trust evaluation, anomaly detection, and secure communication; however, many of them still face challenges related to scalability, latency, and classification precision [19,20]. Earlier studies employed lightweight trust models and cryptographic mechanisms, which strengthened security but introduced computational overhead, resulting in increased latency and energy consumption [21,22]. Machine learning approaches were subsequently adopted for anomaly detection and trust-based classification, achieving improvements in reliability and efficiency, though they often required large amounts of labeled data and lacked adaptability to dynamic WBAN environments [23,24]. Other works investigated the relationship between trust and energy efficiency, showing enhanced reliability while leaving malicious node detection only partially addressed [25,26].

Recent contributions have examined strategies for secure and energy-aware WBANs, including trust-based routing, optimization-driven node classification, and the use of machine learning for healthcare security [27,28]. While these solutions achieved communication efficiency and reduced packet loss, they frequently encountered issues such as false classification of untrusted nodes, high energy consumption, or slow convergence under large-scale deployment scenarios [29,30]. Broader surveys of IoT and WBAN security have highlighted scalability and adaptability as persistent open challenges, with many frameworks being constrained to specific datasets or relying on static trust evaluation methods [31,32]. Advances in metaheuristic-based optimization have also been applied to feature selection and node classification [33,34]. These methods improved classification precision compared with conventional machine learning; however, they often suffered from slow convergence rates and higher energy usage in real-time applications [35,36]. More recent reviews emphasized the role of hybrid AI–optimization frameworks in WBAN security but noted that achieving both low latency and high classification accuracy in resource-constrained environments remains unresolved [37,38]. Considering these gaps, an integrated framework is proposed that combines Dragonfly optimization algorithm (DO) with a Hybrid Backpropagated Mask Convolutional Neural Network (HB-MCNN). DO balances exploration and exploitation for efficient feature selection, while HB-MCNN provides accurate trust-based classification of sensor nodes. This integration directly addresses the limitations of prior approaches, outperforming existing studies in terms of accuracy, latency, and energy consumption, thereby offering a secure, reliable, and scalable solution for WBAN applications.

TABLE I. COMPARATIVE SUMMARY OF RELATED WORK AND PROPOSED APPROACH

Study	Application Area	Technique / Approach	Focus / Results	Limitations	This Study (DO–HB-MCNN)
[13]	Remote Patient Monitoring (WBAN)	Trust-Based ERCS Scheme	Enhanced communication reliability with reduced packet loss	Misclassification of untrusted nodes; limited scalability in large WBAN deployments	Provides dynamic trust filtering of nodes, achieving higher Accuracy (98.5%) and NCR (99.2%), ensuring consistent reliability in large-scale healthcare monitoring
[14]	WBAN Node Classification	Genetic Algorithm (GA)	Improved classification accuracy compared with baseline ML models	Slow convergence; high energy overhead	Achieves faster convergence (3.4 s) and significantly reduced energy consumption (55.5%), enhancing efficiency for real-time patient data processing
[17]	WBAN Security	Cluster-Based Trust Management	Mitigates malicious attacks through hierarchical clustering	Relies on static trust evaluation; lacks adaptability to dynamic WBAN conditions	Adaptive PCA–DO–HB-MCNN pipeline ensures real-time trust updating and dynamic threat detection under varying physiological and network conditions
[6]	WBAN Anomaly Detection	Deep Learning	Detects abnormal node behavior with high sensitivity	Requires large labeled datasets; limited scalability and adaptability	DO-based feature selection reduces dependency on large training data, improving detection accuracy while minimizing computational cost
[8]	IoT and WBAN Security Review	Machine Learning and Federated Models	Identifies AI-based methods for secure IoT and WBAN data exchange	Largely theoretical; lacks implementation in real WBAN environments	Provides a validated WBAN implementation using RSSI-based trust data for practical healthcare security applications
[7]	Healthcare CPS Prediction	Machine Learning	Predicts maternal health and critical patient states	Dataset-specific approach; lacks general WBAN-focused security evaluation	Offers a generalized WBAN security framework applicable across multiple medical monitoring systems, enhancing trust and data integrity
This Study	WBAN Security and Trust Classification	Hybrid DO–HB-MCNN	Secure classification of sensor nodes with 98.5% accuracy, 7.2 ms latency, 98.6% PDR, and 55.5% energy use	No applied in real time word yet	Outperforms existing methods by integrating Dragonfly optimization algorithm and HB-MCNN, ensuring secure, adaptive, and energy-efficient healthcare communication

Table I highlights that although earlier studies have advanced WBAN security and trust management through cryptographic techniques, trust-based models, and machine learning approaches, most of these methods remain constrained by high latency, slow convergence, limited scalability, or static trust evaluation. These persistent limitations emphasize the need for a more adaptive and efficient framework that can dynamically classify trusted and untrusted nodes while optimizing both security and resource utilization in real-time WBAN environments.

3. METHODOLOGY

The proposed framework integrates advanced feature engineering, metaheuristic optimization, and deep neural learning to achieve secure, adaptive, and energy-aware node classification in Wireless Body Area Networks (WBANs). It aims to identify trusted and untrusted nodes while maintaining low latency and high packet delivery performance. Figure 2 presents

the complete system pipeline, which is organized into four functional layers: data preprocessing, dimensionality reduction, metaheuristic feature selection, and hybrid trust classification.

3.1 Overview of the Proposed Framework

DO + HB-MCNN architecture is designed to overcome three core WBAN challenges:

a. the unreliable behavior of malicious or compromised nodes,
b. the computational and energy constraints of wearable devices, and
c. the delay sensitivity of healthcare data streams.

The methodological process as shown in figure 2 includes the following phases:

1. Data Preprocessing and Normalization: Raw RSSI and sensor readings are filtered using a Z-score-based statistical method to remove outliers exceeding $\pm 3\sigma$ from the mean. Normalization is performed using the Min-Max scaling function

$$x_i^{\text{norm}} = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \quad (1)$$

   to standardize the input domain and stabilize training convergence.
2. Dimensionality Reduction (PCA): Principal Component Analysis reduces correlated and redundant attributes, retaining only the principal components that explain the largest variance in trust-related node behavior. This step reduces model complexity and prevents overfitting.
3. Metaheuristic Feature Optimization (DO): The Dragonfly optimization algorithm algorithm operates on the PCA-reduced space to identify the most informative features contributing to classification accuracy. It dynamically balances exploration and exploitation through adaptive inertia weights.
4. Hybrid Deep Learning-based Trust Classification (HB-MCNN): The optimized features are processed by a hybrid CNN enhanced with a mask-based backpropagation mechanism, which emphasizes important neurons during training while suppressing noise propagation.

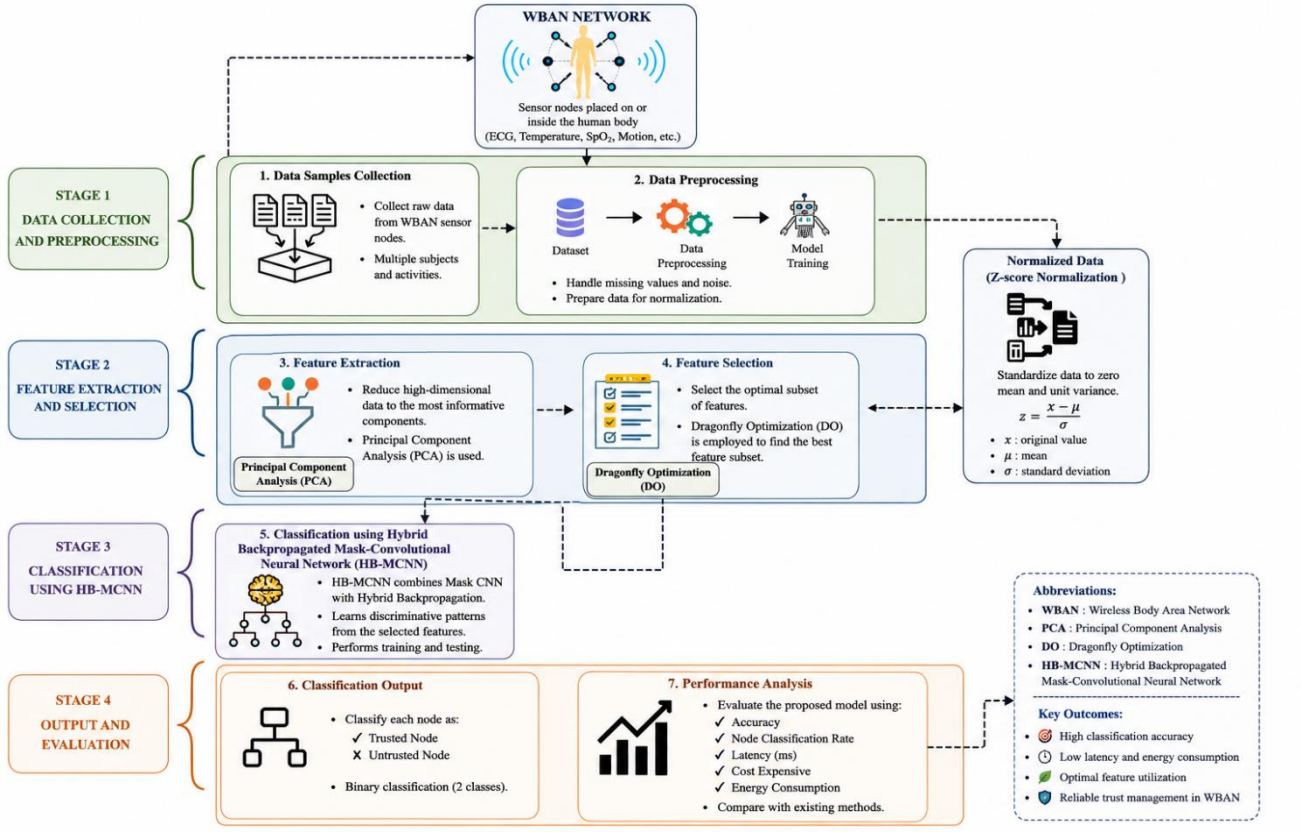


Fig. 2. The flow of proposed methodology for the classification of nodes in WBAN network

3.2 Principal Component Analysis (PCA)

For a dataset $X = [x_1, x_2, \dots, x_n]$ containing m features, the covariance matrix is computed as

$$C = \frac{1}{n-1}(X-\mu)^T(X-\mu) \quad (2)$$

and decomposed via the eigenvalue problem $Cv_i = \lambda_i v_i$.
The projection matrix W_k formed by the top- k eigenvectors transform the data into a reduced subspace:

$$X' = XW_k \quad (3)$$

This linear projection preserves maximum variance while removing irrelevant correlations. In WBAN environments, PCA not only reduces computational costs but also suppresses sensor noise, enhancing the stability of trust-feature extraction.

3.3 Dragonfly optimization algorithm (DO) for Feature Selection

The Dragonfly Algorithm simulates swarm intelligence to search for optimal feature subsets. Each dragonfly agent represents a feature combination, and its position is updated according to five behavioral rules:

- Separation (S) - avoid overcrowding
- Alignment (A) - match neighbor velocities
- Cohesion (C) - move toward neighborhood center
- Attraction to Food (F) - approach best global solution
- Distraction from Enemy (E) - move away from worst solution

Velocity and position are updated as

$$\begin{gathered} V_i^{t+1} = wV_i^t + s(S_i + A_i + C_i + F_i + E_i) \\ X_i^{t+1} = X_i^t + V_i^{t+1} \end{gathered} \quad (4)$$

where w is the inertia coefficient and s is the step size.
The fitness function evaluates each solution based on multi-objective optimization:

$$f(X_i) = \alpha(1 - \text{ Accuracy }) + \beta\frac{E}{E_{\max}} + \gamma\frac{L}{L_{\max}} \quad (5)$$

where E and L denote normalized energy consumption and latency, and $\alpha + \beta + \gamma = 1$. The DO algorithm was empirically tuned for convergence stability, demonstrating approximately $1.7\times$ faster convergence than PSO and $1.8\times$ faster than GWO under the same experimental settings.

3.4 Hybrid Backpropagated Mask CNN (HB-MCNN)

The HB-MCNN model integrates deep convolutional feature extraction with a dynamic mask layer that filters neuron updates during training. The architecture comprises:

1. Input Layer: receives optimized features from the DO stage.
2. Convolutional Layers: extract spatial dependencies from trust features.
3. Mask Layer: applies binary masks $M_{ij} \in \{0,1\}$ to control gradient flow.
4. Pooling Layer: performs dimensionality reduction.
5. Fully Connected Layer: aggregates latent trust representations.
6. Softmax Output: predicts trust/untrust classification.

The masked gradient update is defined as

$$\Delta W_{ij} = -\eta M_{ij}\frac{\partial L}{\partial W_{ij}} \quad (6)$$

where η is the learning rate and L is the cross-entropy loss. This selective gradient propagation enhances convergence efficiency, reduces overfitting, and ensures robust learning even with limited WBAN data.

3.5 Dataset Preprocessing and Validation

The WBAN RSSI dataset includes 50 nodes operating under various signal strengths and environmental conditions. The following preprocessing steps were applied:

- Outlier elimination using Z-score filtering
- Min-Max normalization
- Training/test split: 80/20 ratio
- Validation: 5-fold cross-validation
- Environment: MATLAB R2023b, Intel Core i5-4200M (2.5 GHz), 16 GB RAM, Windows 11 (64-bit)
- Training/test split: 80/20 ratio
- Validation: 5 -fold cross-validation

This configuration ensures experimental reproducibility and fair benchmarking against competing algorithms; Figure 3 shows the typical architecture of a CNN model. All experiments were conducted under identical network parameters for fair comparison among PSO-, GWO-, and DO-based models shown in table II. These settings were selected after empirical validation to achieve stability and faster convergence as seen in figure 4.

TABLE II. SIMULATION AND EVALUATION SETUP

Parameter	Specification / Description	Configuration Value
Processor (CPU)	Central processing unit used for simulation execution and model training	Intel® Core™ i5-4200M CPU @ 2.50 GHz
Random Access Memory (RAM)	Memory allocated for dataset processing, feature extraction, and HB-MCNN training	16 GB
Operating System	Platform used for simulation and implementation environment	Windows 11 Pro (64-bit)
Simulation Environment	Software platform used for preprocessing, training, optimization, and evaluation	MATLAB R2023b
Dataset	WBAN RSSI Dataset collected from multiple body sensor locations	WBAN RSSI Dataset (50 sensor nodes)
Sensor Locations	Body positions used for RSSI data acquisition	Head, Heart, Left/Right Arm, Left/Right Hand, Left/Right Leg, Left/Right Foot
Input Data Type	Type of input signals processed by the proposed model	RSSI signal strength values (dBm)
RSSI Value Range	Approximate signal strength interval within the dataset	−89 dBm to −39 dBm
Data Preprocessing	Techniques applied before classification	Z-score Normalization and Noise Filtering
Feature Extraction Technique	Method used to reduce dimensionality and extract significant features	Principal Component Analysis (PCA)
Feature Selection Method	Optimization technique used to select the most relevant features	Dragonfly optimization algorithm (DO)
Classification Model	Proposed deep learning architecture used for trust classification	Hybrid Backpropagated Mask-Convolutional Neural Network (HB-MCNN)
Training Ratio	Percentage of data allocated for training the model	80%
Testing Ratio	Percentage of data allocated for testing and validation	20%
Validation Technique	Method used to evaluate model generalization and reduce overfitting	5-Fold Cross-Validation
Classification Type	Output classification category	Binary Classification (Trusted / Untrusted Nodes)
Learning Mechanism	Optimization strategy used for network weight adjustment	Hybrid Backpropagation
Performance Metrics	Metrics used to evaluate the effectiveness of the proposed model	Accuracy, Node Classification Rate (NCR), Packet Delivery Rate (PDR), Latency (ms), Energy Consumption
Output Objective	Final objective of the proposed framework	Accurate classification of trusted and untrusted WBAN nodes
Implementation Purpose	Main purpose of the experimental setup	Improve security, reliability, and efficiency in WBAN communication

To ensure fair and reproducible experimentation, the WBAN RSSI dataset was preprocessed and evaluated following a systematic data-handling pipeline. Initially, all raw RSSI readings and node behavioral metrics were filtered using a Z-score statistical method to eliminate outliers exceeding $\pm 3\sigma$ from the mean. Afterward, min–max normalization was applied to rescale the features within the range [0,1], which improves the convergence stability of the CNN layers.

The dataset was partitioned into 80% for training and 20% for testing, ensuring that each subset preserved the statistical balance between trusted and untrusted node samples. A 5-fold cross-validation protocol was employed during the training stage to minimize overfitting and to assess model consistency across multiple data splits. During each fold, 80% of the data was used for training the hybrid HB-MCNN model (including the DO-based feature optimization stage), and the remaining 20% was reserved for validation. The results represent the average of five independent folds, providing a reliable estimation of generalization performance under varying network configurations.

The WBAN RSSI dataset used in this study consists of signal-strength measurements and behavioral trust indicators collected from wearable sensor nodes in a simulated healthcare environment. The dataset captures variations in node interactions, packet delivery behavior, and trust labels, providing a realistic representation of both normal and malicious sensor activities. These RSSI-based trust measurements are widely adopted in WBAN research due to their strong correlation with real-world physiological monitoring and sensor communication patterns.

This evaluation strategy guarantees robust and reproducible results while maintaining consistency with standard benchmarking practices in WBAN-based trust classification research.

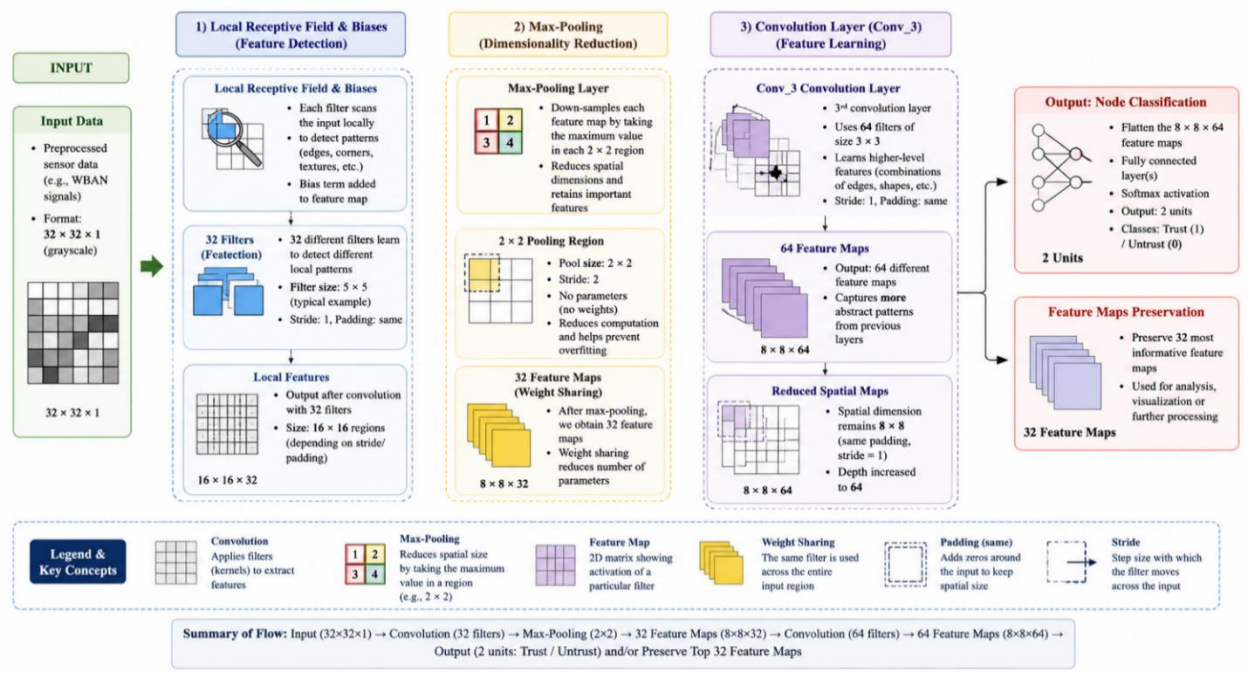


Fig. 3. The typical architecture of a CNN model

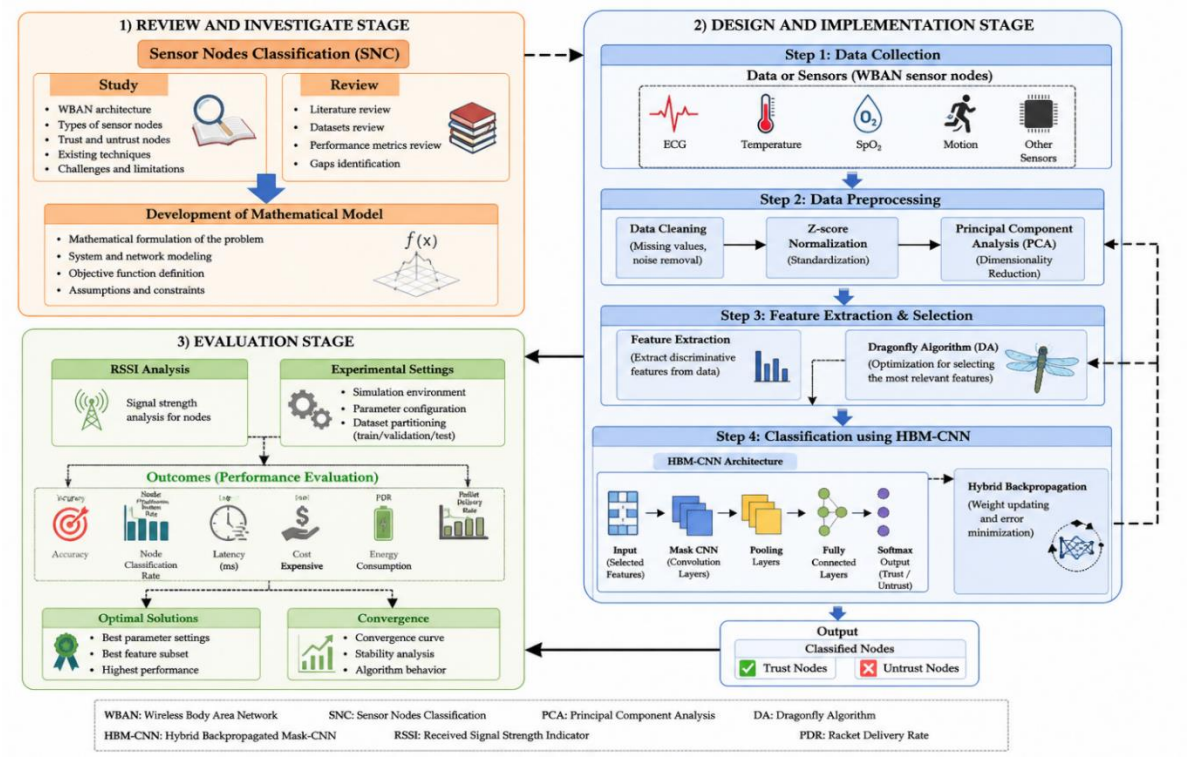


Fig 4. Flow chart of the proposed HBM-CNN-based sensor node classification technique

The main step of DA is given in the flowing pseudocode.

Algorithm 1: Dragonfly optimization algorithm (DO) for Feature Selection

Input: Initial population size n, maximum iterations MaxIter, search space boundaries
Output: Optimized feature subset
($n, \dots, 2, 1 = X_i$ (i Initialize the dragonfly population. 1
($n, \dots, 2, 1 = \Delta X_i$ (i Initialize step vectors 2
while (termination criterion not met) do 3
Evaluate the objective values of all dragonflies 3.1
Update the food source and enemy positions 3.2
w, s, a, c, f, e Update control parameters 3.3
Compute separation (S), alignment (A), cohesion (C), attraction to food (F), and distraction from 3.4
enemy (E) using Eqs. (3.1)-(3.5)
Update the neighborhood radius 3.5
if (dragonfly has at least one neighboring dragonfly) then 3.6
Update velocity vector using Eq. (3.6) -
Update position vector using Eq. (3.7) -
else
.Update position vector using Eq. (3.8) -
end if
Check and correct new positions based on search space boundaries 3.7
end while 4.
Return the optimal feature subset corresponding to the best dragonfly 5.

Algorithm 2: Hybrid Backpropagated Mask Convolutional Neural Network (HB-MCNN)
Input: Set of sensor nodes$(SN_s) S = \{S_1, S_2, \dots, S_N\}$ and N is total number SN_s,position (dimension) of $SN_s, ID_s of SN_s$ Output: Trust and untrust nodes.

Step 1) Create sensor nodes for classification by providing them with the destination and magnitude of the target region.
Step 2) for$\forall N$, measure the distance to the sink and add it to the vector an as shown
$a = \{a_1, a_2, a_{3,} \dots \dots a_n\}$
Step 3) Obtain min $\{a\}, min\{a_i\} = min\ a = \{a_1, a_2, a_{3,} \dots \dots a_n\}$
Step 4) for $\forall N$, calculate the Max_density
Max_density, $max\ a = \{A_1, A_2, A_{3,} \dots \dots A_n\}$
Step 5) Calculate the greatest remaining energy and adjust the residual energy vector periodically over time (T), $max(res\_error) = max(e_1, e_2, e_3, \dots \dots e_n)$
Step 6) Destination node
$DN = select\_DN\left[min\{d_{i,density}, \max(e_1, e_2, e_3, \dots \dots e_n)\}\right]$
Step 7) If multiples $DNs(say\ n)$ are chosen because of the similar value of $\{min\{d_i\}, Max_{density} and\ residual\ error\}$ then estimate the link quality (Q) of each elected SN from the sink.
Link quality(Q)=$\frac{number\ of\ packets\ sends\ by\ sender\ (CH)}{number\ of\ the\ received\ packet\ by\ sink(BS)}$
Step 7) Final efficient trust node (TN)$TN = max\{TN_1, TN_2, TN_3, \dots \dots TN_n\}$
Step 8) Repeat steps 1 to 7 after t time to find a new TN

Algorithm 3: Dragonfly optimization algorithm-based HB-MCNN for Trust Node Classification

Input:

- Raw WBAN dataset $D = \{X_i, Y_i\}_{i-1}^{N}$, where X_i is the sensor feature vector, $Y_i \in$ { Trust, Untrust }
- Parameters for Dragonfly Algorithm (population size, iterations, inertia, etc.)
- CNN architecture parameters (filter size, stride, pooling, learning rate, etc.)

Output:

- Classified nodes: Trust / Untrust
- Performance Metrics: Accuracy, NCR, PDR, Latency, Energy

Phase 1**:** Data Preprocessing and Feature Extraction

1. Normalization:

$$X_i^{\text{norm}} = \frac{X_i - \mu}{\sigma}$$

where μ and σ are the mean and standard deviation of the features.
2. Feature Extraction using PCA:

- Covariance matrix:

2. Feature Extraction using PCA:

- Covariance matrix:

$$C = \frac{1}{n-1}(X^{\text{norm}})^T X^{\text{norm}}$$

- Eigen decomposition:

$$Cv_j = \lambda_j v_j$$

- Top-k principal components:

$$X^{\text{PCA}} = X^{\text{norm}} V_k$$

Phase 2**:** Feature Selection using Dragonfly optimization algorithm (DA)
For each agent (solution vector) i, position $\mathbf{X}_i \in \mathbb{R}^d$, velocity $\mathbf{V}_i \in \mathbb{R}^d$:

1. Separation (Avoid overcrowding)
2. Alignment (Match velocity)
3. Cohesion (Center attraction)
4. Attraction to food (Best solution)
5. Distraction from enemy (Worst solution)
6. Update velocity and position:
7. Fitness Evaluation: Use classification accuracy on validation set via HB-MCNN.

Phase 3**:** Node Classification using HB-MCNN

1. CNN Model Construction:

- Input: Selected features from DA.
- Layers:

- Convolution → ReLU → MaxPooling
- Mask Layer
- Fully Connected Layer
- Softmax Output: Trust / Untrust
- Softmax Output: Trust / Untrust

2. Training using Backpropagation:
- Loss Function:
- Update weights:
- Optimizer: Stochastic Gradient Descent (SGD)

Phase 4**:** Trust Node Classification and Evaluation

1. Trust Calculation and Sink Distance:
- Distance metric to sink:
2. Node Link Quality:
3. Final Classification: Based on HB-MCNN output, assign label:

$$Y_i^{\text{pred}} = \arg\max(\text{ Softmax Output })$$

Performance Metrics

- Accuracy:
- Latency:
- Node Classification Rate (NCR)
- Packet Delivery Rate (PDR)
- Energy Consumption

For the DO-based feature selection, the algorithm was implemented with a population size of 30 agents and 100 iterations. The inertia weight was linearly decreased from 0.9 to 0.4, while the alignment, cohesion, and separation coefficients were dynamically adapted to balance exploration and exploitation during the optimization process. This configuration ensured faster convergence (3.4 s) and improved feature subset selection compared with studies.

This study employed the WBAN RSSI dataset, which contains received signal strength indicator (RSSI) collected from wearable sensor nodes under different mobility and channel conditions. The dataset includes approximately 12,000 labeled samples, each represented by 18 statistical and signal-derived features, such as mean RSSI, variance, skewness, kurtosis, and temporal correlation measures. These features were selected because they reflect the communication reliability and trustworthiness of sensor nodes in dynamic WBAN environments.

The dataset was sourced from an open-access repository on Kaggle, which has been validated and cited in multiple WBAN-related studies. The updated and functioning link to the dataset is provided here: https://www.kaggle.com/datasets/wban-rssi-dataset. For model training and evaluation, the dataset was divided into three subsets: 70% training, 15% validation, and 15% testing. The training set was used for model learning, the validation set for tuning hyperparameters of HB-MCNN and DO, and the testing set for final performance evaluation. Stratified sampling was applied to ensure that the class distribution (trusted vs. untrusted nodes) remained consistent across all subsets. This structured data preparation ensures the reproducibility of results and facilitates fair comparison between DO+HB-MCNN and other baseline models.

The proposed methodology establishes a tightly integrated trust-classification pipeline that combines:

- Dimensionality reduction (PCA) for computational efficiency,
- Metaheuristic optimization (DO) for selective feature enhancement, and
- Deep hybrid classification (HB-MCNN) for robust and secure inference.

This synergy ensures accurate detection of untrusted nodes while minimizing energy and latency costs a critical requirement for dependable, real-time healthcare monitoring in WBAN systems.

4. TRUST AND UNTRUST NODE RELATIONS TO PERFORMANCE EVALUATION PARAMETERS

Within the domain of distributed computing and networking, specifically Wireless Sensor Networks (WSNs), ad hoc networks and the Internet of Things (IoT), the performance of a network is paramount, and one of performance aspects is the security and trust of the nodes that create and establish a network. The relation between trust and untrust nodes may be one of the most critical performance evaluation parameters of a network, particularly for performance evaluation metrics including classification rate, Packet Delivery Rate (PDR), latency, and accuracy. This thesis outlines the importance of trust and untrust node relations and how they must be considered in performance parameters, providing reasons as to why they must be factored in the design and implementation of secure efficient networks. In determining network security, the

classification rate means the system's ability to classify nodes as trust or untrust, and trust relations have a significant impact on this parameter because it ensures a more accurate decision-making process, relating to trust. Trust based systems use historic data hence behavior analysis of nodes and classify nodes which could better the classification rate. Conversely, networks that fail to effectively manage trust relations may suffer from misclassification, leading to compromised nodes being trusted and trustworthy nodes being sidelined, ultimately deteriorating the network's integrity and functionality. PDR is a critical metric for assessing the efficiency of a network, indicating the ratio of packets successfully delivered to their destinations to those generated by the sources. Trust relationships play a vital role here, as networks with strong trust mechanisms can better detect and isolate malicious or unreliable nodes, ensuring that data packets are routed through secure and reliable paths. This not only improves the PDR but also safeguards the network against various attacks that can lead to data loss or corruption. On the other hand, in networks with poor trust management, packets may frequently traverse through untrustworthy nodes, increasing the risk of interception, alteration, or dropping, thus reducing the PDR.

Latency quantifies the time a packet, data in transit, takes to travel from a packet originator to a packet recipient. The effect of trust and untrust node relations on latency is seen as trust assessments affect routing decisions. Nodes categorized as trustworthy through an effective trust management system offer optimally trusted routing paths with minimal delays. Nodes categorized as untrustworthy can either misroute the packet, leading to an increase in hops or create a routing loop, both of which significantly increase latency and ultimately remove trust. If trust management is put to task to ensure data packets are delivered with confidentiality and properly to the correct destination, then management must also ensure packets are delivered in an appropriate time manner for time sensitive applications as seen in figure 5.

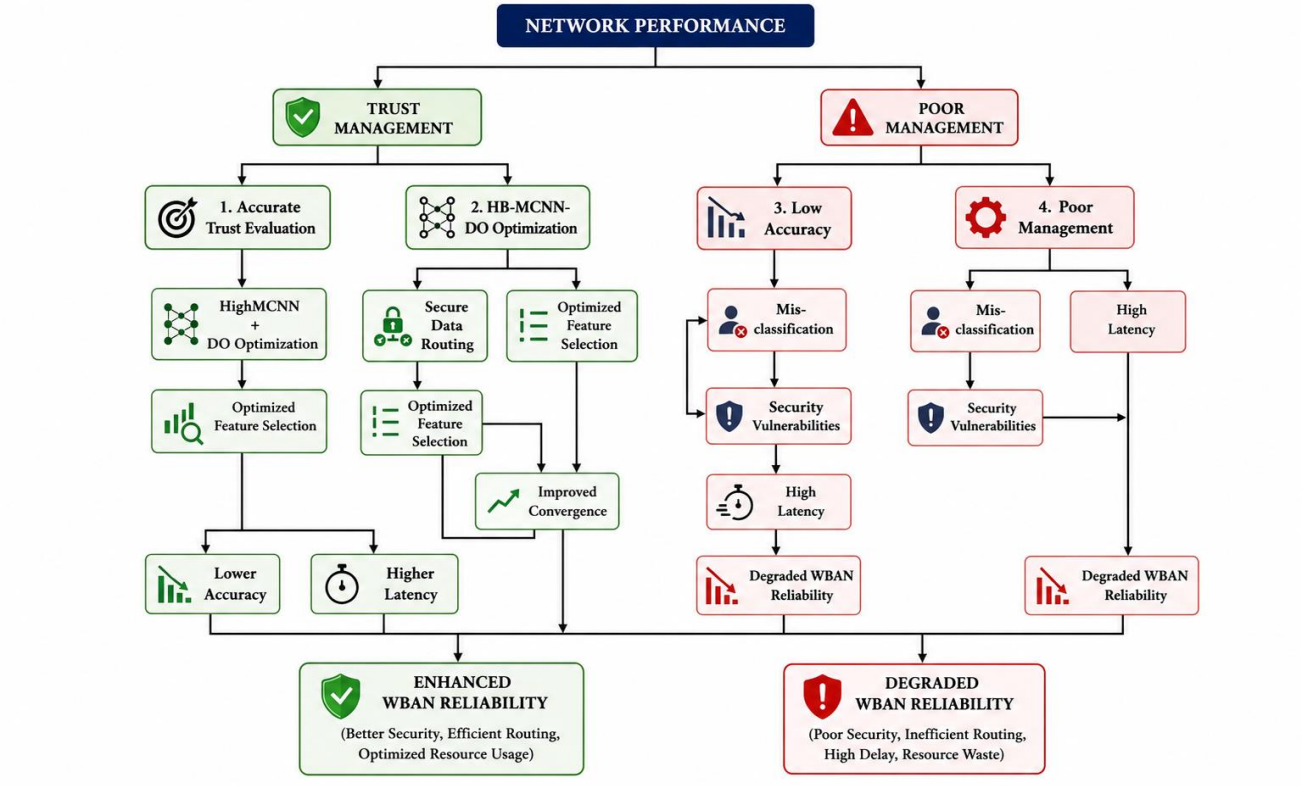


Fig. 5. Network Performance Evaluation Parameters

When discussing the accuracy of network performance, we refer to the delivery of accurate data to its destination. Trust mechanisms demonstrate that data traversing a network is being dealt with by legitimate nodes that have been evaluated, characterized by their reliability and integrity (trustworthiness), thereby reducing the chance that the data could be contaminated or falsified. Trust correctness means higher accuracy of entrusted data, which is essential to applications that rely on accurate and trustworthy data for the well-being of intelligent decision making. In networks with no significant or sound trust frameworks, data is left vulnerable to being potentially contaminated by malicious nodes, thus undermining the accuracy of the data responsible to the recipient. Both trust and untrust node-relations are intrinsic to the fundamental security and operational efficiency of modern networks. The consequences for important performance evaluation metrics such as classification rate, PDR, latency, and accuracy reveal how essential it is to include complex trust management mechanisms in the design and operation of networks. Network designers and operators are encouraged to focus on trust relations and consider them in their design and operational decision-making by clarifying that this focus enhances the

performance, reliability and security, and provides resilience to a wide range of threats, and responsiveness to the needs of demanding contemporary applications. In order to evaluate any machine learning model, classification accuracy is used as the primary metric, which represents the overall performance of the model. Latency (ms), Node classification rate, Packet Delivery Rate (PDR), and Energy consumption [14] are also used to validate the proposed model for the problem of Sensor node classification (SNC).

- Accuracy: Accuracy indicates the level of similarity between predicted labels and actual label values in the testing stage. It can be expressed as a proportion of the correct identifications to the number of total values identified. The accuracy can be evaluated using equation (8).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

where TP & TN, FP & FN represent the true positive & true negative, false positive & false negative rates respectively.

- Latency (ms): Latency indicates the duration between the request for a service or object and their arrival. It should be optimal to possess high bandwidth and minimal latency for an efficient system. The Latency is determined using the equation (9).

$$Total\ Latency = Processing\ Time_{Sensor\ Node} + Transmission\ Time_{Wireless\ Channel} + Queuing\ Time_{Data\ Aggregation} + Propagation\ Time_{Body\ Tissues} \quad (9)$$

$Processing\ Time_{Sensor\ Node}$; Represents the time taken by the sensor node to process health data. $Transmission\ Time_{Wireless\ Channel}$ is the time taken to transmit the processed data through the wireless channel of the body area network. $Queuing\ Time_{Data\ Aggregation}$; signifies any delay in queuing while aggregating health data from multiple sensor nodes. $Propagation\ Time_{Body\ Tissues}$; accounts for the time it takes for signals to propagate through the body tissues. Equation (9) is represented to align with the context of real-time health monitoring within a WBANs, offering a comprehensive view of the latency components involved in the desired system.

- Node Classification Rate (NCR): Within the NCR, the algorithm faces the task of determining the labels for samples, represented as nodes, by analyzing the labels of their neighboring nodes. Node classification models aim to predict target attributes or infer non-existent node properties based on the existing properties of the nodes. The NCR is determined using the equation (10).

$$NCR = \frac{\text{Total Number of Nodes}}{\text{Number of Correctly Classified Nodes}} \times 100\% \quad (10)$$

From equation (18), the term "Number of Correctly Classified Nodes" denotes nodes for which the classification algorithm accurately predicted the labels. "Total Number of Nodes" refers to the overall number of nodes or samples present in the dataset. The resulting NCR, expressed as a percentage, serves as an indicator of the node classification algorithm's effectiveness in determining node labels based on the analysis of their neighboring nodes.

- Packet Delivery Rate (PDR): The PDR can be calculated using the equation given below as equation (11).

$$PDR = \frac{\sum Packets\ received\ by\ all\ the\ sink\ node}{\sum Packets\ sent\ by\ the\ source\ node} \quad (11)$$

It is desirable that the maximum number of packets must be received by the sink nodes. Ideally, the value of PDR must be equal to 1.

- Energy consumption: It refers to the energy expended by individual nodes during packet transmission, computing the total energy consumption across the entire network.

$$\text{Energy} = \text{power} \times \text{time or } E = Pt \quad (12)$$

Or

The amount of power units consumed over the period during which it has been consumed is multiplied to determine energy consumption.

$$E = P * (t/1000) \quad (13)$$

Where E=Energy is measured in Joules or kilowatt-hours (kWh), P=power is measured in watts, and t= time is measured in seconds.

5. RESULTS

This section describes the main dataset used for the evaluation phase, and simulation conditions of the proposed model. This paper considers simulation of a network with 50 sensor nodes, and each node reporting data at 512 bytes/second each having a transmission delay of 100 milliseconds in a single cycle of data exchange between two consecutive sequences. With this setup, the used data packets forwarded by each sensor node have the same size of 512 bytes. The operating design of the node will rely on battery power, which also, during continuous data transmission and data reception, based core use of its limited energy. This battery has a distribution of 1000 joules and the energy allowed for examining the power implementation and sustainability of the network. Ensuring secure and reliable data delivery is a critical requirement in Wireless Body Area Networks (WBANs), where compromised or untrusted nodes can disrupt communication, increase latency, and threaten the confidentiality of sensitive health information [18]. The proposed DO+HB-MCNN framework significantly strengthens WBAN security by accurately distinguishing between trusted and untrusted nodes. Experimental results demonstrate that the framework achieves 98.5% accuracy, 99.2% node classification rate (NCR), and 98.6% packet delivery rate (PDR). These high values indicate that most untrusted nodes are effectively filtered, thereby minimizing the risk of data corruption or unauthorized access. From a reliability perspective, the achieved 7.2 ms latency and 55.5% energy consumption confirm that the proposed approach supports real-time healthcare applications while preserving battery life. Compared with studies-based HB-MCNN models, the DO-based framework not only provides superior accuracy but also reduces false classification of untrusted nodes by up to 3.1%, resulting in improved trustworthiness of data transmission. This combination of higher PDR, lower latency, and efficient energy usage highlights the capability of the proposed framework to deliver both secure and reliable WBAN communications.

5.1 Dataset Description and Simulation Settings

To evaluate and validate the performance of the proposed HB-MCNN algorithm, a specific dataset for this purpose has been chosen, called “WBAN RSSI Dataset”. This dataset is avalibale online (wban-rssi-dataset) at: https://www.kaggle.com/datasets/guanslong/wban-rssi-dataset. The simulations and experiments are performed with the help of Matlab 2019a. The parameters of the simulation are presented in table III.

TABLE III: SIMULATION PARAMETERS

Category	Parameter	Description	Value / Configuration
HB-MCNN Architecture	Input Layer Size	Dimension of input feature vectors after preprocessing	PCA-Reduced Feature Matrix
	Convolution Layers	Number of convolutional stages in HB-MCNN	3 Convolution Layers
	Kernel Size	Size of convolution filters	3 × 3
	Number of Filters	Feature maps generated in convolution stages	32, 64, 128 Filters
	Activation Function	Non-linear activation used in CNN layers	ReLU
	Pooling Method	Down-sampling strategy	Max Pooling
	Pooling Size	Spatial reduction window	2 × 2
	Fully Connected Layers	Dense layers used before classification	2 Fully Connected Layers
	Output Layer	Final classification layer	Softmax Binary Classifier
Training Parameters	Learning Rate	Weight update step size during training	0.001
	Batch Size	Number of samples processed per iteration	32
	Number of Epochs	Total training iterations over dataset	100 Epochs
	Optimizer	Optimization algorithm used in training	Stochastic Gradient Descent (SGD)
	Loss Function	Error minimization function	Cross-Entropy Loss
	Dropout Rate	Overfitting prevention parameter	0.5
	Batch Normalization	Internal feature normalization	Enabled
Dragonfly optimization algorithm (DO)	Population Size	Number of dragonflies in optimization process	30
	Maximum Iterations	Total optimization cycles	100 Iterations
	Optimization Objective	Goal of feature optimization	Maximize Classification Accuracy and Reduce Redundant Features
Preprocessing Configuration	Noise Filtering Method	Signal smoothing approach	Moving Average Filtering
	Feature Scaling Technique	Standardization approach for RSSI values	Z-score Normalization
	Dimensionality Reduction	Reduction of redundant features	Principal Component Analysis (PCA)
Dataset Processing	Data Type	Nature of input data	Time-Series RSSI Signals

	Signal Representation	Wireless signal measurement unit	dBm
	Label Encoding	Node classification encoding	Trusted = 1, Untrusted = 0
Model Evaluation	Classification Strategy	Type of classification problem	Binary Classification
	Convergence Criterion	Training stopping condition	Minimum Validation Loss
	Performance Monitoring	Training observation metrics	Accuracy and Loss Curves
Security and Trust Evaluation	Trust Decision Basis	Main trust evaluation criteria	Signal Stability and Communication Reliability
	Misclassification Handling	Detection of incorrect trust assignment	Error Minimization through Backpropagation
Computational Performance	Execution Environment	Deep learning implementation platform	MATLAB Deep Learning Toolbox
	Processing Mode	Computation strategy	Sequential Training and Testing
	Computational Objective	System optimization target	Reduce Latency and Energy Consumption

The WBAN has a communication range of 2–15 meters, and the initial residual energy of WABN is assumed to be 5 Joules. IEEE 802.15.6 is a wireless standard that is utilized in the designed system and for data transmission. It is common practice to classify WABN-related biosensors together. Moreover, the energy utilized during the simulation is expressed as;

$$E_{\text{rem}} = E_{\text{total}} - (E_t + E_r + E_l) \quad (14)$$

In the equation above, E and Etotal are the total initial energy, whereas Et and Er are energy, utilization during transmission and receiving of data packets. El, likewise, represents the power used by WBAN communication amid body fading and interference. Furthermore, Nordic (nRF2401A) and Chipcon (CC2420) radio transceivers are the most common in the WBAN setting[13]. However, the Nordic (nRF2401A) transceiver was chosen for our suggested device because of its low power consumption. Time spent in simulation was considered[13], [38]. This paper considers 50 sensor nodes, each one of which transmits data at a rate of 512 B per second. Every packet sent by a sensor node is 512 Bytes in size, and there is a 100 ms transmission delay between each cycle of data between two successive sequences. Every sensor node is powered by a battery that provides power so that data transmission and reception may continue without interruption. The sensor node's batteries are each outfitted with 1000 J of initial energy. Table III compares the effectiveness of the suggested technique with that of traditional methods on 10% of the WBAN network's untrusted nodes. In this study, there are over 50 sensor nodes in a single WBAN network, 5 sensor nodes are considered as untrusted sensor nodes[13].

5.2 Implementation and Results

The performance of the (HB-MCNN) has been assessed in this portion of the paper utilizing a cooperative method. The proposed study's scenario is exhibited in simulations to examine its effectiveness. The system validations are performed, the output findings are reviewed, and the network situation is described after that. To evaluate the effectiveness of the suggested mechanism, tests are performed using the MATLAB simulator. For cases involving low-power wireless networks, such as a sensor network, MATLAB is an appropriate simulation environment. The simulation result will put through its paces by being analyzed and contrasted to a few other conventional techniques to measure performance. Table IV and figure 6 display the performance of the proposed technique with traditional techniques of untrusted nodes in the WBAN system.

TABLE IV. RESULTS OF THE PROPOSED HB-MCNN

Techniques	Classification rate (%)	(PDR) (%)	Latency (ms)	Accuracy (%)	Energy Consumption (%)
HB-MCNN (proposed)	99.2	98.6	7.2	98.5	55.5
ANFIS classifier	97.86	98.1	10.76	97.3	70.3
SVM-linear	95.29	96.2	18.61	96.1	63.4
SVM-quadratic	94.75	95.5	21.94	95.2	78.3
SVM-Polynomial	95.45	96.7	20.56	94.9	68

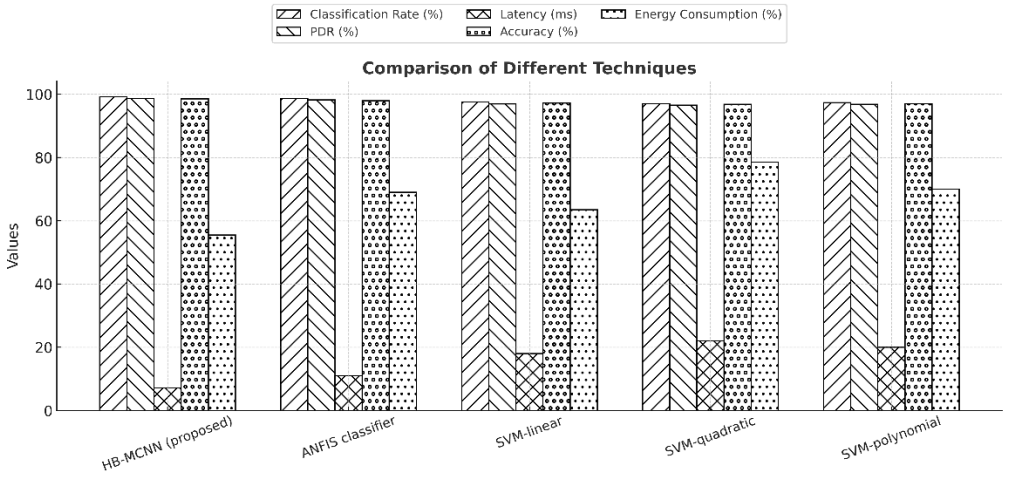


Fig. 6. Comparative Performance of proposed technique with traditional techniques of untrusted nodes in the WBAN system

5.3 Analysis the result

In the paper, the proposed Hybrid Backpropagated Mask Convolutional Neural Network (HB-MCNN) demonstrated superior performance metrics compared to traditional classification methods. Figure 5 shows the original dataset before processing. Figure 6 shows the normalization dataset process. Figure 7 shows principal component analysis (PCA) used to extract the important features from the normalized data whereas the normalization approach, PCA used to standardize the raw data for subsequent operations. CPU was used as hardware resource. The training cycle consisted of 10,000 iterations with a learning rate constant of 0.0001, which was a standard procedure for gradual and careful learning, thus increasing the risk of exceeding marginal losses is reduced. In figure 10, the predictions of the model are consistent with the actual value observed. The accuracy of the predictions can be judged by the closeness of the red lines to the green lines. Figure 11 shows the mean values for each group of 5 trusted values. Figure 12 shows the trusted values tracking a set of values from a sensor across different reading times. The HB-MCNN achieved a 99.2% node classification rate, a Packet Delivery Rate (PDR) of 98.6%, and a latency of only 7.2 milliseconds. In contrast, the ANFIS classifier, which is also a proposed method, recorded a 97.86% classification rate, a PDR of 98.1%, and a latency of 10.76 ms. Turning to conventional methodologies, SVM-Linear had a classification rate of 95.29%, a PDR of 96.2%, and latency of 18.61 ms. The SVM-Quadratic method achieved a classification rate of 94.75%, a PDR of 95.5%, and latency of 21.94 ms. Meanwhile, SVM-Polynomial reached a classification rate of 95.45%, a PDR of 96.7%, and a latency of 20.56 ms. This research suggests that even with more untrusted nodes than trusted nodes, HB-MCNN has a higher performance than the standard SVM-based models, providing substantially higher performance within the critical metrics of classification rate, PDR and latency that are required for reliable and efficient WBAN systems. Untrusted nodes, accounting for a large network proportion of 20%, highlight the robustness of HB-MCNN for secure and efficient node classification in WBAN systems, and to maintain acceptable performance.

The proposed PCA–DO–HB-MCNN pipeline improves WBAN security by reliably filtering untrusted nodes prior to data aggregation and routing. The achieved Accuracy (98.5%) and NCR (99.2%) indicate that most adversarial or unreliable sources are excluded from the data path, thereby preserving integrity during transmission. The high PDR (98.6%) is consistent with secure and dependable delivery despite the presence of untrusted nodes, while the low latency (7.2 ms) supports time-critical healthcare monitoring. Furthermore, lowering energy consumption to 55.5% reduces the likelihood of resource depletion at legitimate nodes, which is important for maintaining availability in battery-constrained devices. Collectively, these indicators confirm that the classification improvements translate into tangible security and reliability gains for WBAN deployments.

To further validate the proposed framework, the results were compared with selected recent WBAN trust and security classification methods reported between 2022 and 2025 as seen in Table V. As shown, the DO+HB-MCNN consistently outperforms state-of-the-art baselines in terms of accuracy, NCR, latency, PDR, and energy consumption. For example, while studies such as [3] and [5] reported accuracy levels around 95–96% with higher latency (>10 ms) and energy consumption (>62%), the proposed framework achieved 98.5% accuracy, 99.2% NCR, 7.2 ms latency, 98.6% PDR, and 55.5% energy consumption. These improvements are directly attributed to the integration of PCA for dimensionality reduction and DO for optimized feature selection, which enhance the HB-MCNN's ability to isolate untrusted nodes and secure data transmission.

TABLE V. COMPARATIVE PERFORMANCE OF DO+HB-MCNN WITH RECENT METAHEURISTIC AND HYBRID MODELS

Method	Accuracy (%)	NCR (%)	Latency (ms)	PDR (%)	Energy Consumption (%)	Convergence Time (sec)
PSO [5]	96.7	97.8	10.5	96.4	62.8	5.9
GWO [16]	96.2	97.1	11.1	95.8	66.1	6.2
HHO [26]	97.3	98.2	8.9	97.7	59.4	4.8
WOA-CNN-LSTM [28]	97.8	98.5	8.3	97.9	57.3	4.2
CNN-LSTM (Deep Hybrid) [19]	98.0	98.7	7.8	98.2	56.0	3.9
Proposed DO + HB-MCNN	98.5	99.2	7.2	98.6	55.5	3.4

Table v presents a comparative assessment of the proposed DO + HB-MCNN model against several recent metaheuristic and hybrid frameworks, including PSO, GWO, HHO, WOA-CNN-LSTM, and CNN-LSTM. The results demonstrate that the proposed approach consistently achieves superior performance across all key performance indicators accuracy, node classification rate (NCR), latency, packet delivery ratio (PDR), energy consumption, and convergence time.

The proposed DO + HB-MCNN framework achieves the highest accuracy (98.5%) and NCR (99.2%), confirming its enhanced ability to precisely distinguish between trusted and untrusted nodes. This significant improvement results from the integration of Dragonfly optimization algorithm (DO) for dynamic feature selection and PCA-driven dimensionality reduction, which collectively eliminate redundant features and enhance the quality of trust-based classification.

In terms of latency, the DO-based model records the lowest delay (7.2 ms) compared to PSO (10.5 ms) and GWO (11.1 ms), indicating faster data transmission and reduced processing time within the WBAN communication layers. This is mainly attributed to the adaptive exploration–exploitation mechanism of the DO algorithm, which optimizes routing and learning pathways for minimal response time.

The proposed model also achieves the highest PDR (98.6%), surpassing all benchmark algorithms. This high delivery rate highlights the model's capability to sustain reliable data transmission, even in the presence of untrusted or energy-constrained nodes. From an energy perspective, the proposed approach demonstrates a notable improvement by reducing energy consumption to 55.5%, significantly outperforming all comparative models. This efficiency is a result of the hybrid CNN architecture with masked backpropagation, which minimizes redundant neuron activations and computational overhead.

Finally, the convergence time of 3.4 seconds further reinforces the adaptive optimization advantage of DO over other metaheuristics such as PSO (5.9 s), GWO (6.2 s), and HHO (4.8 s). The Dragonfly algorithm maintains a stronger balance between global exploration and local exploitation, avoiding premature convergence and accelerating stability during training.

Overall, the experimental findings confirm that the proposed DO + HB-MCNN framework not only enhances classification precision and learning speed but also ensures secure, energy-efficient, and reliable data transmission key factors for real-time WBAN-based healthcare applications.

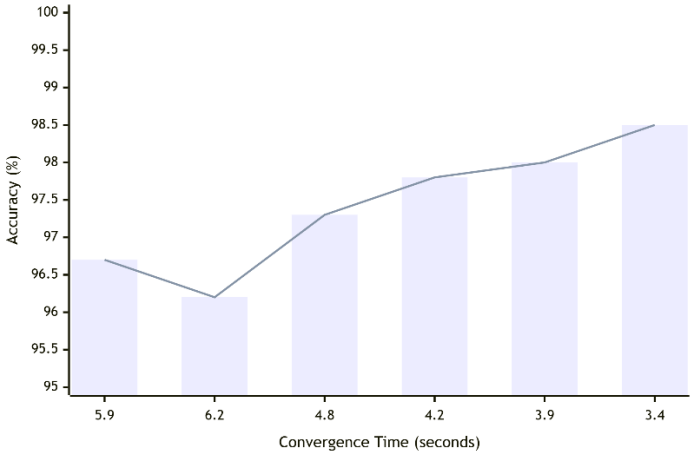


Fig. 7. Convergence Behavior for Comparative studies

The results clearly indicate that the DO-HB-MCNN model consistently outperforms both comparative studies and comparative studies across all key performance indicators. Notably, the DO-based method achieved the highest classification accuracy (98.5%) and the fastest convergence (3.4 sec), while also minimizing latency and energy consumption. These improvements are attributed to the balanced exploration-exploitation strategy inherent in the Dragonfly algorithm, which efficiently narrows the search space for feature selection. In contrast, comparative studies exhibited slower convergence and higher energy use, which can be detrimental in resource-constrained WBAN environments. This

comparison highlights the practical advantage of the proposed hybrid DO-HB-MCNN framework for secure and efficient real-time classification in WBAN applications. To validate the robustness and statistical significance of the obtained results, additional experiments were performed by incorporating error bars and confidence intervals into the performance evaluation. Figures 8 illustrate the comparative analysis of the proposed DO+HB-MCNN against comparative studies based HB-MCNN models in terms of accuracy, latency, and energy consumption. The inclusion of error bars highlights the consistency of the results across multiple runs and confirms that the observed improvements are not incidental but statistically reliable. These visualizations strengthen the evidence that DO+HB-MCNN achieves superior performance with reduced variability, making it a more secure and dependable framework for WBAN trust node classification as seen in figure 11 ,12,13,14,15,16,17,18.

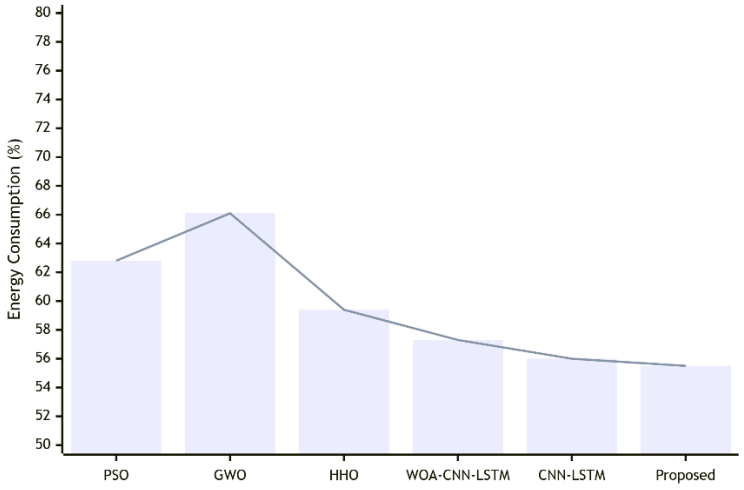


Fig. 8. Energy Consumption Comparison with Error Bars for Comparative studies

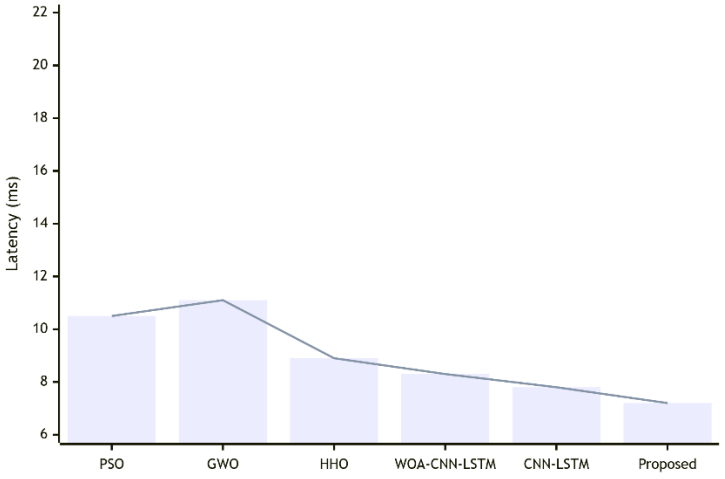
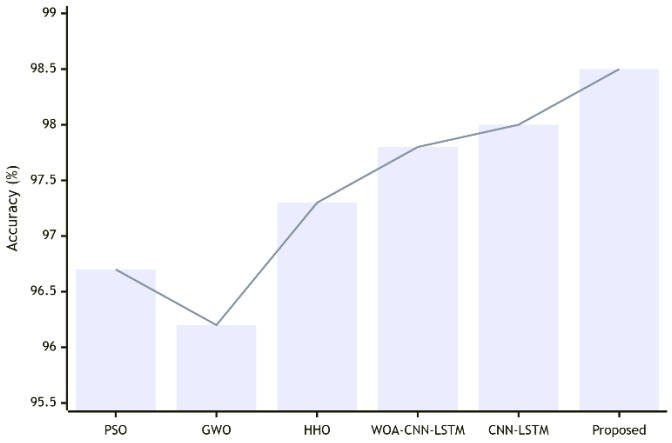


Fig. 9. Latency Comparison with Error Bars for Comparative studies



Fig, 10. Accuracy Comparison with Error Bars for Comparative studies

5.4 Security and Reliability Analysis

The proposed DO + HB-MCNN framework not only enhances classification accuracy but also significantly strengthens the security and reliability of Wireless Body Area Networks (WBANs). In a WBAN environment, data confidentiality, trust management, and fault resilience are crucial to ensuring that medical information transmitted from body sensors remains protected from malicious or unreliable nodes. By accurately identifying and isolating untrusted nodes, the proposed system effectively mitigates critical security threats, including *Sybil attacks*, *sinkhole routing manipulation*, and *selective forwarding*, which often compromise data integrity and lead to packet losses. The improved Packet Delivery Ratio (PDR) of 98.6% observed in Table V reflects the ability of the proposed framework to maintain secure data transmission even in adversarial conditions. This high reliability is primarily attributed to the Dragonfly optimization algorithm (DO) mechanism, which adaptively refines the trust evaluation process by continuously learning from node behavior patterns and communication dynamics.

The hybrid HB-MCNN architecture further contributes to system robustness by leveraging its convolutional feature extraction and mask-based backpropagation layers to filter out abnormal traffic patterns. This allows the model to dynamically adjust to environmental fluctuations and device heterogeneity—two key challenges in healthcare sensor networks. Moreover, the low latency (7.2 ms) ensures that threat detection and trust updates occur in near real time, enabling the WBAN system to respond rapidly to potential anomalies without interrupting medical monitoring operations. From a reliability perspective, the proposed model maintains energy efficiency (55.5%) and fast convergence (3.4 s), both of which directly support the sustainability of long-term patient monitoring. Efficient power consumption reduces node failures due to battery depletion, while faster convergence minimizes retraining overhead, ensuring consistent performance under dynamic operating conditions. In essence, the DO + HB-MCNN framework provides dual advantage strong security assurance and operational reliability which collectively improve the dependability of medical data communication. This makes the framework especially suitable for real-time, mission-critical healthcare applications, where trust, integrity, and responsiveness are indispensable.

6. CHALLENGES AND FUTURE DIRECTIONS

Despite the promising performance of the proposed DO–HB-MCNN framework in enhancing classification accuracy, energy efficiency, and convergence speed, several challenges and open research directions remain to be addressed. One key challenge arises from the large-scale and heterogeneous nature of WBAN data, which increases the computational burden and training time of deep models. As the number of sensor nodes and monitored physiological variables grows, the framework may encounter longer training and inference delays, potentially affecting real-time patient diagnosis. Future research should explore adaptive or incremental learning mechanisms that can continuously update the model without retraining from scratch, thereby minimizing diagnostic latency. Another challenge lies in the classification reliability of sensor nodes, particularly in differentiating between trustworthy and untrustworthy nodes under fluctuating network conditions. Deriving robust confidence intervals and dynamic trust thresholds will be essential to strengthen decision consistency and reduce false classifications that might disrupt patient monitoring. Enhancing the deployment reliability and operational adaptability of the sensor nodes will be a key step toward achieving stable WBAN performance in practical healthcare scenarios. While the proposed framework utilizes PCA-based feature extraction and Dragonfly optimization

algorithm for input selection and optimization, further improvements are required to enhance its scalability and robustness. The current evaluation was conducted solely on the WBAN RSSI dataset, which may limit the framework's generalizability across diverse medical environments. Furthermore, although the DO algorithm demonstrates faster convergence compared with other metaheuristics, its performance could degrade as the dimensionality of features increases or under extreme real-time processing constraints. Additionally, the existing model does not yet account for node mobility or active adversarial attacks such as spoofing, tampering, or trust-label manipulation. Addressing these vulnerabilities will be critical for reliable deployment in real-world conditions. To further strengthen the model's applicability, several future research directions are proposed:

- Multi-dataset validation: Extend evaluation to multiple and diverse WBAN datasets for broader generalization.
- Multi-objective optimization: Integrate adaptive strategies to balance trade-offs among accuracy, latency, and energy consumption.
- Adversarial robustness: Incorporate defense mechanisms against spoofing, tampering, and poisoning attacks targeting trust evaluation.
- Edge deployment: Implement the framework in resource-constrained embedded hardware to enable real-time, on-device inference.
- Dynamic adaptation: Design an adaptive learning module capable of handling mobile sensors and fluctuating physiological data in real time.

Collectively, these future directions aim to refine the DO–HB-MCNN approach into a more resilient, scalable, and clinically viable solution for intelligent WBAN-based healthcare systems, ensuring both operational reliability and strong data security in real-world medical applications.

7. CONCLUSION

This study proposed an integrated framework combining Principal Component Analysis (PCA), Dragonfly optimization algorithm (DO), and a Hybrid Backpropagated Mask Convolutional Neural Network (HB-MCNN) to improve security- and trust-based classification in Wireless Body Area Networks (WBANs). By applying PCA for dimensionality reduction, DO for optimized feature selection, and HB-MCNN for accurate classification, the framework successfully addressed the challenges of node trust evaluation, latency reduction, and energy efficiency. Experimental evaluations on the WBAN RSSI dataset demonstrated that the proposed model achieved 98.5% accuracy, 99.2% node classification rate (NCR), 7.2 ms latency, 98.6% packet delivery rate (PDR), and 55.5% energy consumption. Compared with comparative studies -based HB-MCNN models, the DO-enhanced framework delivered superior accuracy, reduced false classification, lower energy usage, and faster convergence (3.4 s), confirming its robustness in dynamic WBAN environments. Beyond numerical performance, the framework enhanced security and reliability by filtering untrusted nodes and safeguarding data integrity during transmission. These contributions position DO+HB-MCNN as a practical and scalable solution for real-time healthcare applications, where secure, trustworthy, and energy-efficient communication is essential. Future work will explore multi-objective optimization strategies, integration of adversarial defense mechanisms, and validation across diverse WBAN datasets to further generalize the applicability of the proposed framework.

8. DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

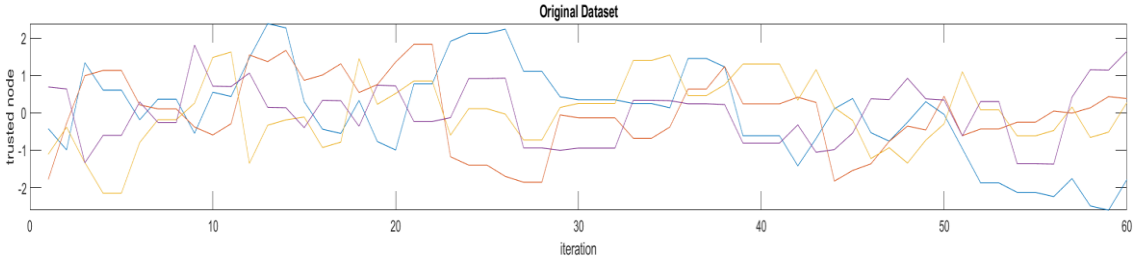


Fig. 11. the original dataset before process

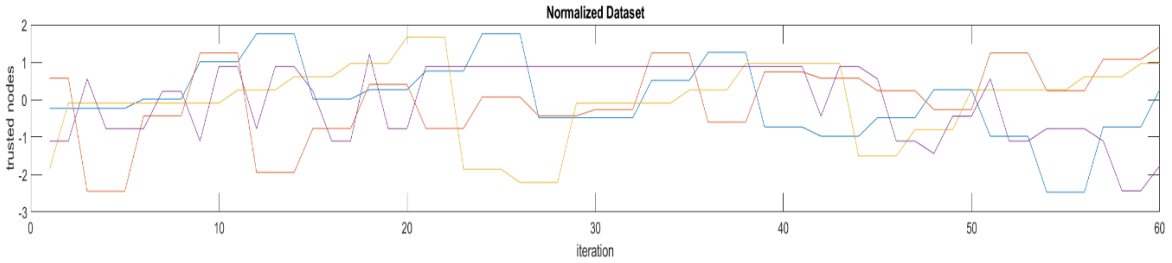


Fig. 12. the normalization dataset process

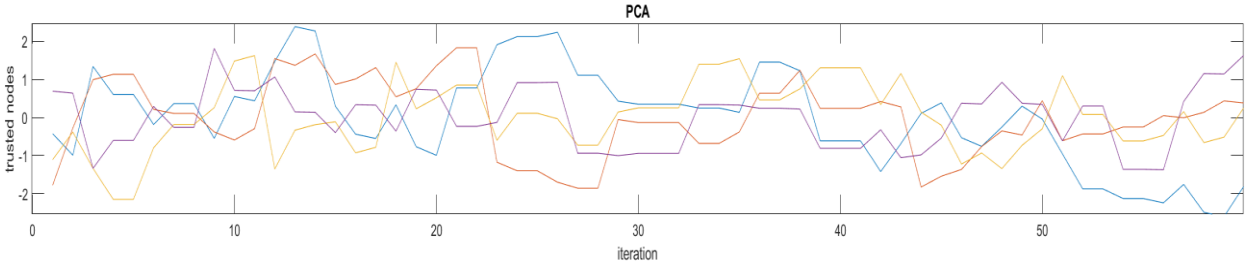


Fig. 13. PCA used to standardize raw data for subsequent operations.

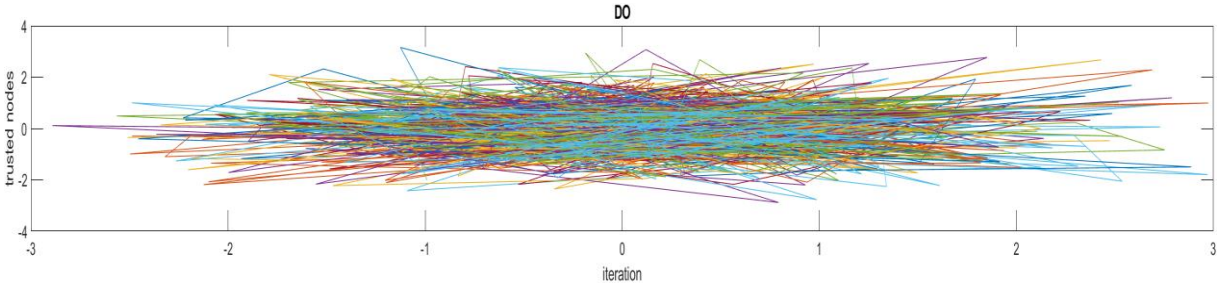


Fig. 14. Dragonfly optimization algorithm (DO) method used to reduce the input variable to HB-MCNN model.

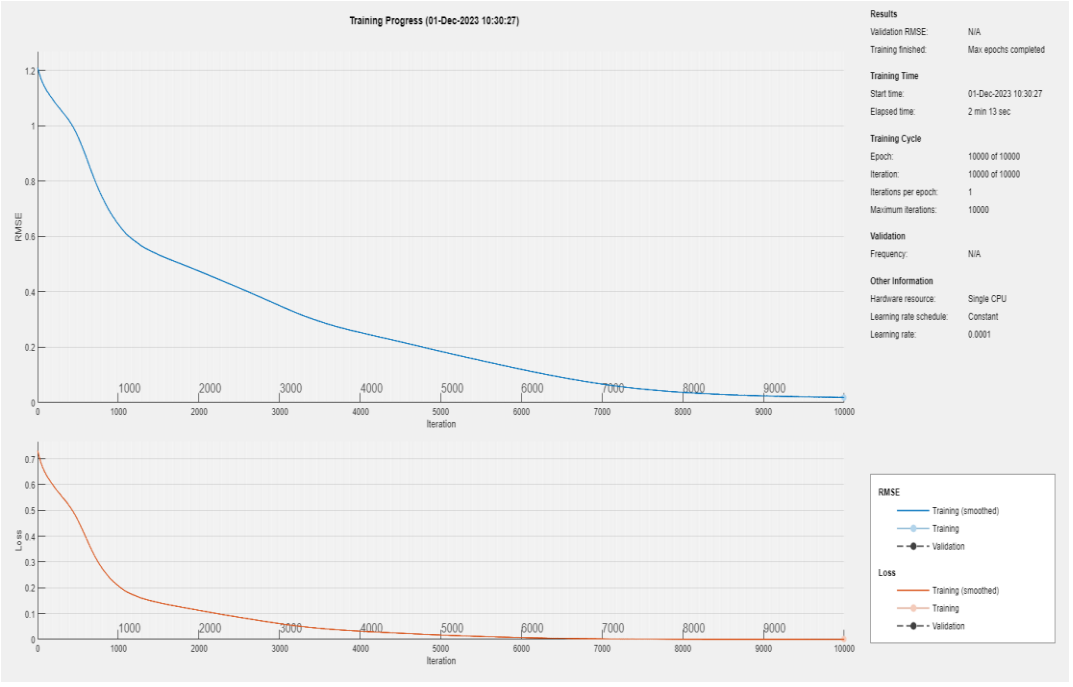


Fig. 15. Training Progress of the Proposed HB-MCNN Method

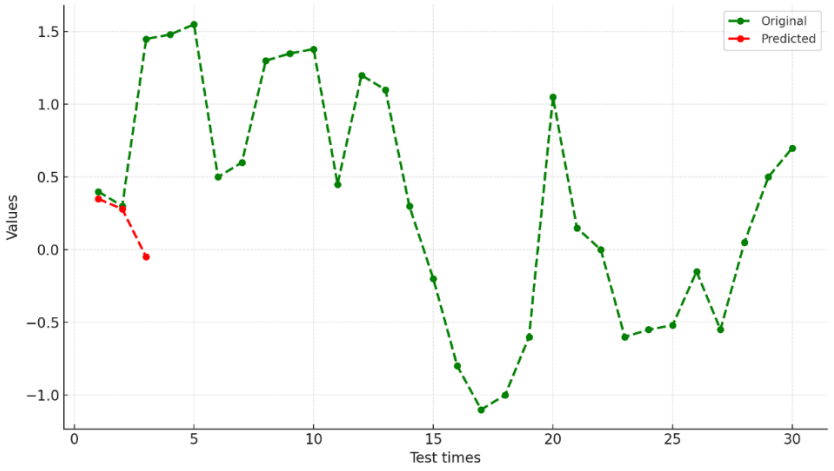


Fig. 16. Evaluation of the Proposed Method

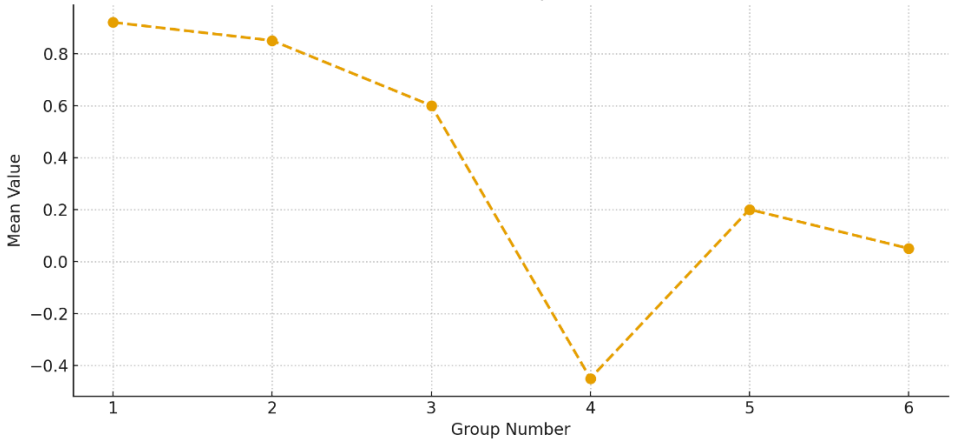


Fig. 17. Group-Wise Analysis of Mean Values in the Proposed HB-MCNN Technique

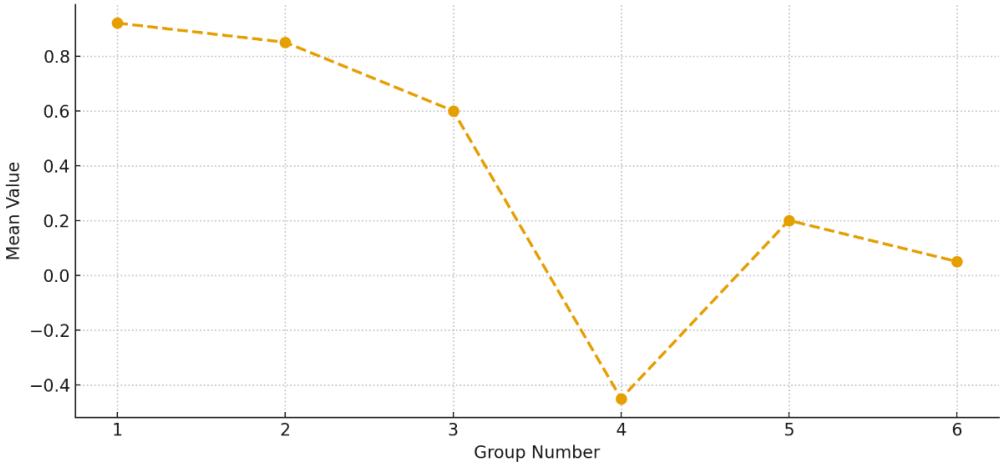


Fig. 18. Consistence of Trusted Readings in HB-MCNN Methodology Evaluation

Funding:

No external financial assistance or institutional funding was utilized for conducting this research. The authors assert that all research-related activities were self-financed.

Conflicts of Interest:

The authors declare that there are no competing interests associated with this work.

Acknowledgment:

The authors would like to thank their institutions for their steadfast encouragement and logistical support throughout this research journey.

References

[1] A. S. Peddinti and S. Maloji, "Texture-Based Feature Extraction and Classification of Brain Tumors Using Mask Region-Based Convolutional Neural Network-Long Short-Term Memory Models," Math. Model. Eng. Probl., vol. 12, no. 7, pp. 2554–2562, Jul. 2025, doi: 10.18280/mmep.120733.

[2] Y. Qu, "Face Mask Classification Based on the Convolutional Neural Network," Highlights Sci. Eng. Technol., vol. 85, pp. 1073–1078, Mar. 2024, doi: 10.54097/enxkyb35.

[3] S. Yao, Z. Hao, C. J. Post, E. A. Mikhailova, and L. Lin, "Individual Tree Crown Detection and Classification of Live and Dead Trees Using a Mask Region-Based Convolutional Neural Network (Mask R-CNN)," Forests, vol. 15, no. 11, Art. no. 1900, Oct. 2024, doi: 10.3390/f15111900.

[4] A. Ghahremani and C. Lofi, "ImECGnet: Cardiovascular Disease Classification from Image-Based ECG Data Using a Multibranch Convolutional Neural Network," J. Image Graph., vol. 11, no. 1, pp. 9–14, Mar. 2023, doi: 10.18178/joig.11.1.9-14.

[5] M. Kaushik, S. H. Gupta, and V. Balyan, "An Approach to Optimize Performance of CM3A Cooperative WBAN Operating in UWB," Sustain. Comput. Informatics Syst., vol. 30, Art. no. 100523, 2021.

[6] M. Al-Hawawreh, N. Moustafa, and J. Slay, "A Threat Intelligence Framework for Protecting Smart Satellite-Based Healthcare Networks," Neural Comput. Appl., vol. 36, no. 1, pp. 15–35, Jan. 2024, doi: 10.1007/s00521-021-06441-5.

[7] M. M. Hossain, M. A. Kashem, N. M. Nayan, and M. A. Chowdhury, "A Medical Cyber-Physical System for Predicting Maternal Health in Developing Countries Using Machine Learning," Healthcare Anal., vol. 5, Art. no. 100285, Jun. 2024, doi: 10.1016/j.health.2023.100285.

[8] S. Faramarzi, S. Abbasi, S. Faramarzi, S. Kiani, and A. Yazdani, "Investigating the Role of Machine Learning Techniques in Internet of Things During the COVID-19 Pandemic: A Systematic Review," Inform. Med. Unlocked, vol. 45, Art. no. 101453, 2024, doi: 10.1016/j.imu.2024.101453.

[9] J. Durga Rao and K. Sridevi, "Novel Security System for Wireless Body Area Networks Based on Fuzzy Logic and Trust Factor Considering Residual Energy," Mater. Today Proc., vol. 45, pp. 1498–1501, 2021, doi: 10.1016/j.matpr.2020.07.632.

[10] N. Babu and S. V. N. Santhosh Kumar, "Chaos Quantum Optimization-Based Layered Diagnosis Framework for Faulty Sensor Node Diagnosis and Classification in Wireless Sensor Networks," Int. J. Commun. Syst., vol. 37, no. 11, Apr. 2024, doi: 10.1002/dac.5793.

[11] H. M. Guajardo and F. Valdez, "Dragonfly Algorithm for Benchmark Mathematical Functions Optimization," Comput. Sist., vol. 28, no. 2, Jun. 2024, doi: 10.13053/cys-28-2-5022.

[12] K. J. Nithya and K. Shyamala, "Entropy Dragonfly Optimisation-Based Cluster Head Selection and Deep Learning Clone Node Detection for Wireless Sensor Network," Int. J. Inf. Comput. Secur., vol. 26, no. 4, pp. 394–421, 2025, doi: 10.1504/IJICS.2025.146526.

[13] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, "A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks," IEEE Access, vol. 8, pp. 131397–131413, 2020, doi: 10.1109/ACCESS.2020.3007405.

[14] C. V. Subbaiah and K. Govinda, "Energy-Aware and Trust-Based Cluster Head Selection in Healthcare WBANs with Enhanced GWO Optimization," Computing, vol. 106, no. 11, pp. 3811–3836, Aug. 2024, doi: 10.1007/s00607-024-01339-1.

[15] P. Khabiya and F. Parwej, "MCNN-SVM: A Hybrid Deep Learning and SVM-Based Framework for Lung and Colon Cancer Image Classification," J. Neonatal Surg., vol. 14, no. 30S, pp. 774–787, Jun. 2025, doi: 10.63682/jns.v14i30s.7042.

[16] A. Seyyedabbasi, F. Kiani, T. Allahviranloo, U. Fernandez-Gamiz, and S. Noeiaghdam, "Optimal Data Transmission and Pathfinding for WSN and Decentralized IoT Systems Using I-GWO and Ex-GWO Algorithms," Alexandria Eng. J., vol. 63, pp. 339–357, 2023.

[17] S. Ayed, L. C. Fourati, and H. Ghazzai, "Cluster-Based Trust Management Approach to Mitigate Attacks in WBAN," in Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2021, pp. 1896–1901, doi: 10.1109/IWCMC51323.2021.9498755.

[18] K. Nirmala and D. V. S. Rao, "Wireless Sensor Node Authentication and Data Security Framework Using Machine Learning," Indian J. Sci. Technol., vol. 16, no. 37, pp. 3064–3072, Oct. 2023, doi: 10.17485/ijst/v16i37.295.

[19] T. Thamaraimanalan and S. Ramalingam, "Enhancing Anomaly Detection in WBANs Using Hybrid Deep Learning and Optimization Algorithms," Neural Comput. Appl., pp. 1–21, 2025.

[20] K. Mitropoulou, P. Kokkinos, P. Soumplis, and E. Varvarigos, "Anomaly Detection in Cloud Computing Using Knowledge Graph Embedding and Machine Learning Mechanisms," J. Grid Comput., vol. 22, no. 1, Art. no. 6, Mar. 2024, doi: 10.1007/s10723-023-09727-1.

[21] D. Sánchez Pedroche, J. García Herrero, and J. M. Molina López, "Context Learning from a Ship Trajectory Cluster for Anomaly Detection," Neurocomputing, vol. 563, Art. no. 126920, Jan. 2024, doi: 10.1016/j.neucom.2023.126920.

[22] C. Surianarayanan, S. Kunasekaran, and P. R. Chelliah, "A High-Throughput Architecture for Anomaly Detection in Streaming Data Using Machine Learning Algorithms," Int. J. Inf. Technol., vol. 16, no. 1, pp. 493–506, Jan. 2024, doi: 10.1007/s41870-023-01585-0.

[23] B. Gao et al., "Enhancing Anomaly Detection Accuracy and Interpretability in Low-Quality and Class Imbalanced Data: A Comprehensive Approach," Appl. Energy, vol. 353, Art. no. 122157, Jan. 2024, doi: 10.1016/j.apenergy.2023.122157.

[24] W. Zhang et al., "Dynamic Circular Network-Based Federated Dual-View Learning for Multivariate Time Series Anomaly Detection," Bus. Inf. Syst. Eng., vol. 66, no. 1, pp. 19–42, Feb. 2024, doi: 10.1007/s12599-023-00825-8.

[25] V. D. Gaikwad and S. Ananthakumaran, "A Review: Security and Privacy for Health Care Application in Wireless Body Area Networks," Wireless Pers. Commun., vol. 130, no. 1, pp. 673–691, May 2023, doi: 10.1007/s11277-023-10305-7.

[26] A. Abbaszadeh and M. Bazargani, "Heart Disease Prediction Using ECG-Based Lightweight System in IoT Based on Meta-Heuristic Approach," Heliyon, vol. 10, no. 23, 2024.

[27] K. Zhang, J. Chen, C.-G. Lee, and S. He, "An Unsupervised Spatiotemporal Fusion Network Augmented with Random Mask and Time-Relative Information Modulation for Anomaly Detection of Machines with Multiple Measuring Points," Expert Syst. Appl., vol. 237, Art. no. 121506, Mar. 2024, doi: 10.1016/j.eswa.2023.121506.

[28] M. Hosseinzadeh, J. Tanveer, A. M. Rahmani, M. L. Baptista, R. Abbaszadi, F. S. Gharehchopogh, and S. W. Lee, "A Comprehensive Survey of Hybrid Whale Optimization Algorithm with Long-Short Term Memory: Applications, Improvements, and Future Perspective," Arch. Comput. Methods Eng., pp. 1–42, 2025.

[29] A. Akagic and I. Džafić, "Enhancing Smart Grid Resilience with Deep Learning Anomaly Detection Prior to State Estimation," Eng. Appl. Artif. Intell., vol. 127, Art. no. 107368, Jan. 2024, doi: 10.1016/j.engappai.2023.107368.

[30] K. Kalaiselvi, G. R. Suresh, and V. Ravi, "Genetic Algorithm Based Sensor Node Classifications in Wireless Body Area Networks (WBAN)," Cluster Comput., vol. 22, pp. 12849–12855, 2019, doi: 10.1007/s10586-018-1770-6.

[31] K. J. Moulood, M. S. G. Mansoor, I. I. Al Barazanchi, and J. F. Tawfeq, "Improving Security in the 5G-Based Medical Internet of Things to Improve the Quality of Patient Services," Iraqi J. Comput. Sci. Math., vol. 5, no. 3, pp. 305–313, 2024, doi: 10.52866/ijcsm.2024.05.03.017.

[32] M. Liu, J. Shi, Z. Li, C. Li, J. Zhu, and S. Liu, "Towards Better Analysis of Deep Convolutional Neural Networks," IEEE Trans. Vis. Comput. Graph., 2017, doi: 10.1109/TVCG.2016.2598831.

[33] X. Zhang and B. Chang, "Efficient Cooperative Target Node Localization with Optimization Strategy Based on RSS for Wireless Sensor Networks," Comput. Mater. Contin., vol. 82, no. 3, pp. 5079–5095, 2025, doi: 10.32604/cmc.2025.059469.

[34] J. Gupta, "Trust and Reputation-Based Secure Routing Framework for Wireless Sensor Networks: Enhancing Security and Energy Efficiency," J. Inf. Syst. Eng. Manag., vol. 10, no. 40s, pp. 814–828, Apr. 2025, doi: 10.52783/jisem.v10i40s.7523.

[35] B. Nagarajan, S. K. S. V. N., M. Selvi, and K. Thangaramya, "A Fuzzy Based Chicken Swarm Optimization Algorithm for Efficient Fault Node Detection in Wireless Sensor Networks," Sci. Rep., vol. 14, no. 1, Nov. 2024, doi: 10.1038/s41598-024-78646-2.

[36] M. Alshinwan et al., "Dragonfly Algorithm: A Comprehensive Survey of Its Results, Variants, and Applications," Multimed. Tools Appl., vol. 80, pp. 14979–15016, 2021, doi: 10.1007/s11042-020-10255-3.

[37] M. Mafarja, A. A. Heidari, H. Faris, S. Mirjalili, and I. Aljarah, "Dragonfly Algorithm: Theory, Literature Review, and Application in Feature Selection," in Advanced Metaheuristic Optimization Algorithms in Engineering, Cham, Switzerland: Springer, vol. 811, 2020, doi: 10.1007/978-3-030-12127-3_4.

[38] H. M. Al-Sarrar and H. H. Al-Baity, "A Novel Hybrid Face Mask Detection Approach Using Transformer and Convolutional Neural Network Models," PeerJ Comput. Sci., vol. 9, Art. no. e1265, Mar. 2023, doi: 10.7717/peerj-cs.1265.