International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2169-2176
Journal homepage: http://iieta.org/journals/ijsse

Optimizing IoT Intrusion Detection and Attack Classification via WOA-Based Feature Reduction and Boosting Algorithms

Manar Bashar Mortatha[1,2*], Dhahir Abdulhade Abdulah[1]

[1] Department of Computer Science, College of Science, Diyala University, Baqubah 32001, Iraq
[2] Department of Computer, College of Education for Pure Sciences, Wasit University, Al-Kut 52001, Iraq

Corresponding Author Email: scicomphd232407@uodiyala.edu.iq

https://doi.org/10.18280/ijsse.151019

Received: 19 September 2025
Revised: 20 October 2025
Accepted: 25 October 2025
Available online: 31 October 2025

Keywords:
IoMT, intrusion detection, WOA feature selection, XGBoost, LightGBM, class imbalance

ABSTRACT

Intrusion detection on the Internet of Medical Things (IoMT) must contend with heterogeneous, multi-protocol traffic (Wi-Fi, MQTT, BLE) and severe class imbalance that undermines per-class reliability. This study proposes a hybrid two-stage pipeline that integrates Whale Optimization Algorithm (WOA) for feature reduction with boosting-based classifiers (XGBoost, LightGBM). Stage-1 performs binary detection (Normal vs. Attack); Stage-2 classifies attack types across 14 classes. Using the CICIoMT2024 dataset, WOA consistently prunes ~40–60% of features, cutting training time by up to ~68% while preserving near-perfect Stage-1 detection. On multi-class evaluation, WOA+XGBoost attains Accuracy = 0.9976, Macro-F1 = 0.9599, and Weighted-F1 = 0.9977, with stable per-class F1-scores (≈ 0.90-1.00) and only a modest dip on UDP. WOA+LightGBM remains competitive (Accuracy = 0.9864; Weighted-F1 = 0.9859) but exhibits larger variance on minority classes (e.g., VulScan ≈ 0.34). On the BLE subset, WOA selects ~12-13 of ~21 features with negligible accuracy loss and lower detection latency. The findings demonstrate that WOA-driven reduction is an effective cost-preserving step for IoMT intrusion detection, and that XGBoost provides more stable per-class performance under imbalance. We discuss CPU-only deployment feasibility (with batching/quantization) and outline targeted remedies class balanced reweighting, focal loss, and hierarchical classification to further improve rare-class detection.

1. INTRODUCTION

The Internet of Medical Things (IoMT) is an important revolution in health care since it allows real-time monitoring, diagnosis, and treatment in the hospital, wearable, and home. IoMT makes healthcare more convenient and effective, but on the other hand, also brings out new attack surfaces due to its heterogeneity, constrained devices, and multi-protocol communications, including Wi-Fi, MQTT, and Bluetooth. Attackers generally leverage these weaknesses, and this may result in a threat to patient safety, a threat to data privacy, and/or a threat to service availability.

To counter the increasing security threats in IoMT, intelligent IDSs using machine learning (ML) and deep learning (DL) have been proposed by researchers. To this end, the CICIoMT2024 dataset was presented as a realistic dataset to the community for the development and evaluation of these models. It consists of network traffic generated by 40 medical IoT devices and over 18 attacks, classifiers such as DOS, DDOS, Recon, MQTT, and Spoofing, that operate under different protocol conditions [1].

Recent studies obtained encouraging results on CICIoMT2024 through ensemble and boosting methods [2]. As an example, tree-based ensembles with feature reduction (RF/XGBoost via RFECV) achieved weighted-F1 ≈ 0.995 on CICIoMT2024, highlighting the strength of boosting/ensembles on this dataset [2]. Similarly, a data-augmentation, feature-engineering, deep-ensemble, voting/stacking pipeline (Transformer/LSTM/DCNN → meta-learner) reported ~99% accuracy on CICIoMT2024 and strong cross-device generalization [3]. However, performance typically drops when moving from binary detection to fine-grained multi-class attack-type classification on CICIoMT2024; for instance, a Transformer with time encodings reached ~0.73 accuracy (F1 ≈ 0.67) in the multi-class setting using CICIoMT2024 baselines [4].

To cope with these limitations, we propose a hybrid model that couples the Whale Optimization Algorithm (WOA) for feature selection with an ensemble that performs binary detection followed by hierarchical attack-type classification to improve accuracy, reduce computational cost, and enhance interpretability.

1.1 Research objectives and contributions

This paper presents a hybrid model for IoMT intrusion detection that is based on:

1. Feature selection based on WOA to solve the high-dimensional CICIoMT2024 dataset.
2. accurate detection and classification by boosting

classifiers (XGBoost and LightGBM).
3. Accuracy and execution time-based performance evaluation approach.

1.2 Key contributions

1. WOA-driven feature reduction for CICIoMT2024 that removes 40–60% of features while preserving near-perfect Stage-1 detection.
2. A protocol-aware design that treats Wi-Fi/MQTT and BLE slices separately, with tailored WOA settings and feature subsets for each protocol family.
3. A systematic comparison of XGBoost and LightGBM on full vs WOA-reduced features for both binary and multi-class IoMT intrusion detection.
4. A detailed CPU-only runtime and latency analysis demonstrating the feasibility of deploying the proposed pipeline on resource-constrained IoMT edge gateways.

2. RELATED WORK

2.1 IoT intrusion detection feature selection

Efficient feature selection is crucial in IoT to reduce issues such as redundancy, high dimensionality, and low detection, as highlighted in recent studies. The study by Ayad et al. [5] suggested a combination of a filter-wrapper approach to anomaly-based intrusion detection in IoT. By using SMOTE on class imbalance, it was then shown that a hierarchical system, which first classifies the network packets as normal or attack, and then the type of the attack, can achieve high accuracy (99.82–100%) with fast ID time on BoT-IoT, TON-IoT, and CIC-DDoS2019 datasets [5].

To improve the feature selection of the dimensionality reduction methods, we proposed a two-stage feature selection method suitable for IoT [6], and the method filtered the features more effectively [6] and achieved better detection performance.

Going deeper into metaheuristic search, a hybrid WOA-GWO has been recently used for feature selection in IoT intrusion detection. The model deals with global and local search optimization; global optimal convergence can be achieved early, and local optimal refinement can occur later, addressing the shortcomings of single-algorithm approaches [7].

Additionally, AL-Husseini et al. [8] presented the wrapped feature selection pipeline and implemented the WOA coupled with LSTM classifiers. When applied to CICIDS 2017 and NSL KDD datasets, this technique helped in a reduction in the number of features (78 → 68), leading to the effect of WOA in terms of dimensionality reduction and classification effectiveness (DDoS detection accuracy was 99.62%) [8].

2.2 IoT security with boosting algorithms

Ensemble methods and boosting classifiers have been highly promising in IoT-based IDS. Adewole et al. [9] considered the ensemble approaches that involve the combination of RF, AB, XGBoost, LightGBM, and CatBoost. Their results indicated that XGBoost performed better than others in binary and multi-class IoT intrusion detection, in addition to providing explainability [9].

The study by Hafid et al. [10] also suggested a high-performance cyber security architecture based on fine-tuning of an XGBoost classifier boosted with SHAP Explanations (XAI) and late fusion. The model performed with 0.97 accuracy and perfect recall (1.00), presenting a rather balanced performance, and was deemed suitable for IoMT applications where security is a priority [10].

2.3 New deep learning and feature engineering methods

Enriching traditional ML, DL, and representation learning has formed two spots of light in IDS research:

Inspired by a genetic sequence classification problem with heterogeneous inputs, the MIAE architecture introduces a feature-selection layer to efficiently handle inputs from multiple sources. When combined with Random Forest, MIAEFS achieved up to 96.5% accuracy on the NSL-KDD and UNSW-NB15 datasets, using compact models (< 1 MB) and delivering fast detection times (~1.7×10^{-6} s) [11].

Jouhari et al. [12] presented an effective IDS model comprising of χ^2 feature selection combined with a CNN–BiLSTM classification model. On UNSW NB15, the performance was 97.90% for binary tasks and 97.09% for multi-class classification with low inference time, which is suitable for resource-limited IoT devices [12].

Ghubaish et al. [13] introduced LEMDA, a lightweight means decreases in accuracy of feature engineering. LEMDA outperformed state-of-the-art algorithms on several IoT datasets by significantly enhancing F1-scores (average: + 34%) and reducing both detection and training times, a feature that is particularly useful for deployable IoT systems [13].

2.4 Summary of gaps and positioning of our work

Building on the gaps summarized in Table 1, our work addresses the key gap that no prior study has systematically combined WOA-driven feature reduction with XGBoost and LightGBM on protocol-specific medical IoT data (BLE vs. Wi-Fi/MQTT). We propose a unified framework that uses WOA to optimize feature subsets and then trains boosting classifiers—XGBoost and LightGBM—on the CICIoMT2024 dataset, rigorously evaluating both classification performance and runtime efficiency for scalable, protocol-specific IoT intrusion detection.

Table 1. Summary of gaps in the literature and positioning of our work

Domain	Gaps Addressed
Feature Selection	Hybrid methods like WOA–GWO or filter–wrapper excel on generic datasets but have not been applied to multi-protocol IoMT datasets like CICIoMT2024.
Boosting Models	Boosting algorithms show strong performance, yet require evaluation on heterogeneous, multi-class IoMT data with feature reduction.
DL and Feature Engineering	Advanced architectures like MIAEFS and LEMDA exist but are yet to be tested for real IoMT datasets combining Wi Fi, MQTT, and BLE traffic with boosting classifiers.

2.5 Recent IJSSE contributions on IoT/IoMT security

Recent works in the International Journal of Safety and Security Engineering (IJSSE) have addressed IoT and IoMT security from complementary angles. Mutleg et al. [14]

provided a comprehensive review of cyber-attacks targeting IoT systems and corresponding security measures, emphasizing the evolving threat landscape and generic defense strategies. Other work by the same group developed DL-based intrusion detection models for IoT technology and explicitly studied the trade-off between detection accuracy and computational complexity on the ToN-IoT dataset [15]. Additional IJSSE contributions explore machine- and deep-learning-based intrusion detection in specialized environments, such as enhanced SVM/RNN classifiers for underwater wireless sensor networks and intelligent intrusion detection frameworks based on federated learning for distributed IoT networks [16, 17]. In contrast to these works, our study provides a protocol-aware, WOA-driven feature reduction framework combined with boosting classifiers and a detailed runtime analysis on CICIoMT2024

3. METHODOLOGY

In this section, we detail the four main stages of our proposed approach: data description and splitting, preprocessing, feature selection via WOA, and training of boosting classifiers. Tables summarize key parameters and results, and a workflow diagram illustrates the pipeline.

3.1 Data description and splitting

As summarized in Table 2, the CICIoMT2024 dataset includes 40 devices (25 real and 15 simulated), spans Wi-Fi, MQTT, and BLE protocols, and comprises 18 attack types. For both benign and attack traffic, we adopt an 80/20 train–test split, as detailed in Table 2.

For the Wi-Fi/MQTT branch, the Stage-1 binary detector is trained on 6,564,824 flows, including 504,696 normal and 6,060,128 attack flows, and evaluated on 1,050,981 flows, with 115,599 normal and 935,382 attack flows.

For the BLE branch, the binary detector is trained on 1,230,190 BLE flow records and evaluated on 320,615 BLE flows, of which 3,577 are normal, and 317,038 are attack flows. In the BLE subset analysis, we further focus on the 309,451 BLE attack flows in the test split, including 249,179 DoS flows and 60,272 non-DoS attack flows.

Table 2. Data description and splitting

Feature	Value
No. of Devices	40 totals: 25 real devices and 15 simulated devices (unb.ca)
Protocols Covered	Wi-Fi, MQTT, BLE
No. of Attack Types	18 distinct attacks grouped into five categories: DDoS, DoS, Recon, MQTT, Spoofing (unb.ca)
Data Splits	80% of captured PCAP files for training, 20% for testing (both attacks and benign/profiling)

3.2 Preprocessing

Prior to feature selection and classification, we perform:

1. Missing TTL Imputation: Copy Time_To_Live from profiling data into attack records was missing.
2. Zero-Variance Removal: Drop columns with standard deviation = 0 (e.g., Drate).
3. Categorical Encoding: Apply LabelEncoder to textual fields (e.g., Protocol Type).
4. Numerical Normalization: Standardized continuous features using z-score:

$$x' = \frac{x - \mu_{train}}{\sigma_{train}} \quad (1)$$

where, μ_{train} and σ_{train} are computed on the training subset and applied to the test data.

3.3 Feature selection with WOA

We apply WOA to reduce dimensionality while preserving detection performance. The configuration is:

- Agents (Whales): 30
- Max Iterations: 20
- Early Stopping: halt after 3 generations without improvement
- Fitness Function: see in Eq. (2)

$$Fitness(x) = \alpha\, AUC(X) + \beta\, F1(X) - \lambda \frac{|X|}{P} \quad (2)$$

where,

- AUC(X) is the area under the ROC curve for feature subset X.
- F1(X) is the F1-score (harmonic mean of precision and recall) for X.
- |X| = K is the number of selected features.
- P = is the total original feature count.
- P = 49 for Wi-Fi & MQTT
- P = 23 for BLE
- $\alpha = 0.8$, $\beta = 0.2$ (so $\alpha + \beta = 1$), prioritizing AUC.
- λ is a size-penalty weight tuned on a validation split.

This formulation operationalizes the multi-objective nature of wrapper-based feature selection by jointly optimizing predictive utility and parsimony via a weighted sum of performance metrics and a feature-count penalty [18-21].

3.3.1 Protocol-aware WOA-based feature selection

In the proposed framework, WOA is applied in a protocol-aware manner rather than on a single, merged dataset. Specifically, we run separate WOA searches for the Wi-Fi/MQTT branch and for the BLE branch of CICIoMT2024. This design allows the optimizer to adapt to the distinct traffic characteristics, imbalance levels, and attack distributions of each protocol family instead of enforcing a single "one-size-fits-all" feature subset.

For the Wi-Fi/MQTT branch, WOA starts from the original 49 flow-based features and converges to a compact subset that preserves near-optimal detection performance while substantially reducing dimensionality. For the BLE branch, WOA operates on 23 features and consistently selects 18 features, including traffic statistics (e.g., normalized length, inter-arrival information) and device-level counts (e.g., source/destination attack rates), that are most discriminative between benign and malicious BLE flows.

The fitness function used by WOA is explicitly motivated by IoMT edge deployment, where both predictive performance and computational cost are critical. By jointly maximizing AUC and F1 while penalizing large feature subsets, the optimizer favors solutions that balance accuracy and sparsity. As shown later in the results, the protocol-

specific WOA configurations not only maintain high detection and classification scores but also reduce training and inference time, making the resulting models more suitable for integration into resource-constrained IoMT gateways and hospital edge devices.

The WOA parameters and results are listed in Table 3.

3.4 Binary intrusion detection with boosting

We evaluated two boosting classifiers—XGBoost and LightGBM—on each protocol's dataset using stratified 5-fold cross-validation, hyperparameter tuning, and held-out test splits:

- Datasets:
- Wi-Fi & MQTT + Profiling: 49 original features
- BLE + Profiling: 23 original features
- Training Modes:
- Baseline: trained on the full original feature set.
- WOA-Reduced: retrained on the WOA-selected subsets only (Section 3.3).

As shown in Table 4, both XGBoost and LightGBM achieve very high detection metrics on the full feature sets (Accuracy $\geq$ 0.9972 and AUC = 0.9999), establishing a strong baseline for comparison against the reduced-feature models.

Table 3. WOA-selected feature counts and detection accuracy

Dataset	Original Features	Selected Features	Best Accuracy (%)	Total Runtime (s)
Wi-Fi & MQTT	49	18	99.57	92
Bluetooth (BLE)	23	12	99.96	60

Table 4. Binary detection performance on full feature sets

Model	Accuracy	Precision	Recall	F1-Score	AUC
XGBoost	0.9972	0.9985	0.9970	0.9977	0.9999
LightGBM	0.9975	0.9991	0.9973	0.9982	0.9999

Table 5. Multi-class classification performance on detected-attack samples

Classifier	Accuracy	Macro-F1	Weighted-F1	Lowest Per-Class F1 (VulScan)
WOA+XGBoost	0.9976	0.9599	0.9977	0.74
WOA+LightGBM	0.9864	0.8297	0.9859	0.34

3.5 Multi-class attack classification

As shown in Table 5, approximately 610 931 samples flagged as "Attack" by the binary detector were classified by two flat multi-class models trained on the WOA-selected features, yielding the overall performance metrics below:

The per-class F1-scores in Figure 1 are computed directly from the confusion matrices in Figure 2 (precision/recall derived from TP, FP, and FN per class). Overall, WOA+XGBoost maintains high performance across most classes (≈ 0.90-1.00), with several near-perfect results for high-support categories (e.g., DDoS_Publish_Flood, ICMP) and a modest dip for UDP (~0.78). WOA+LightGBM exhibits greater variability: it remains strong on heavy-traffic classes but drops notably for Ping Sweep (~0.55) and VulScan (~0.35–0.40). These findings indicate that while both boosters are effective on common attack types, XGBoost yields more stable per-class performance; for scarce classes, targeted remedies (e.g., class-balanced reweighting, focal loss, data augmentation, or hierarchical classification) may further improve accuracy.

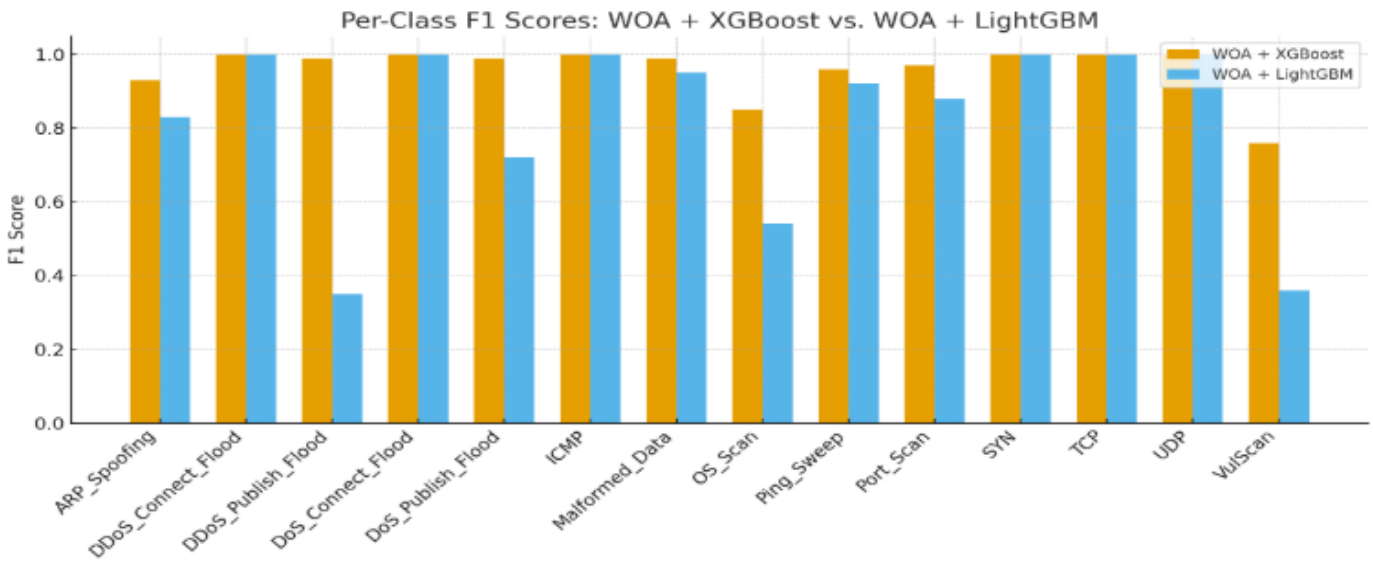
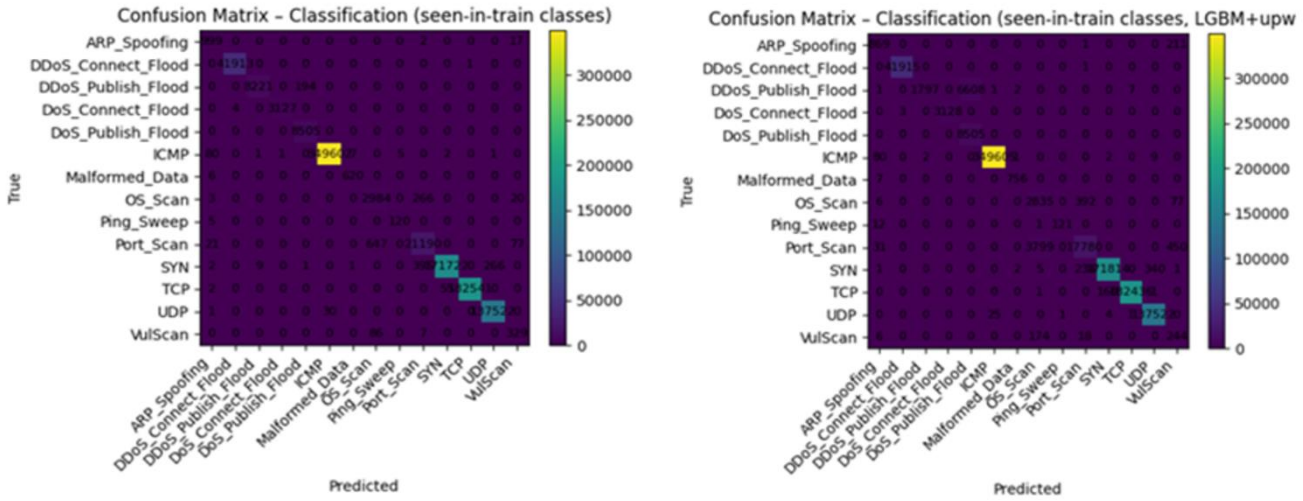


Figure 1. Per-class F1-score comparison (WOA+XGBoost vs. WOA+LightGBM)



(a) (b)

Figure 2. Confusion matrices for Stage-2 multi-class classification: (a) WOA+XGBoost, (b) WOA+LightGBM

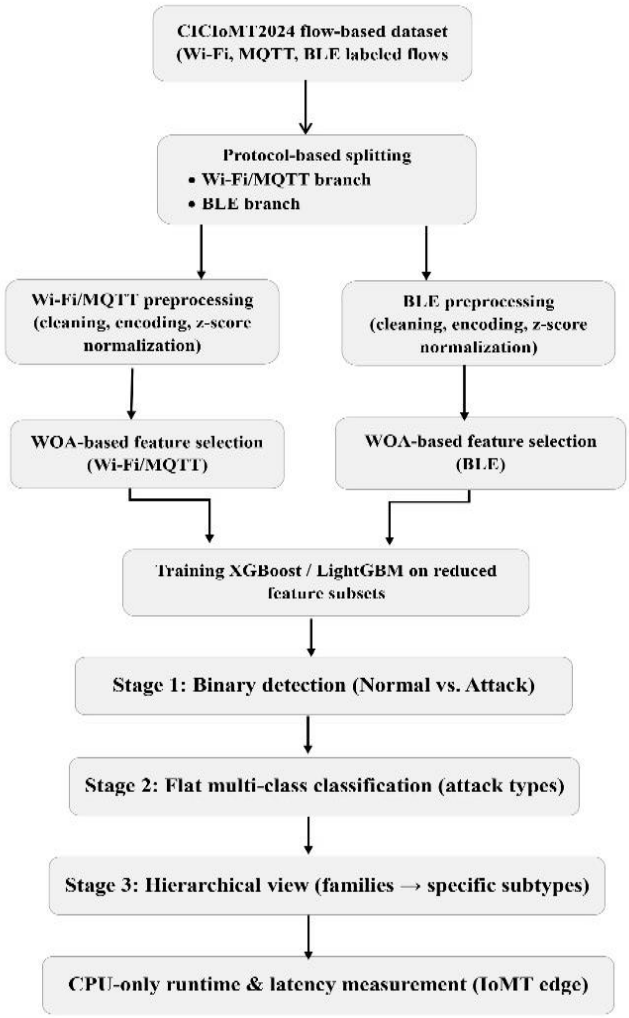


Figure 3. Workflow of the proposed WOA–boosting-based IoMT intrusion detection pipeline on the CICIoMT2024 flow-based dataset

3.6 Workflow diagram

As illustrated in Figure 3, the proposed IoMT intrusion detection pipeline is organized as a sequence of seven stages. We start from the CICIoMT2024 flow-based dataset, which provides labeled Wi-Fi, MQTT, and BLE flows. These flows are then split into two protocol-aware branches (Wi-Fi/MQTT and BLE), each undergoing a dedicated preprocessing chain that includes cleaning, categorical encoding, and z-score normalization.

In the next stage, WOA is applied separately to each branch in order to obtain compact, protocol-specific feature subsets. These reduced feature sets are then used to train XGBoost and LightGBM models in a supervised manner. The detection process itself is structured into three conceptual classification stages: Stage-1 binary detection (Normal vs. Attack), Stage-2 flat multi-class classification over the individual attack types, and an optional hierarchical view in which attacks are grouped into broader families before distinguishing specific sub-types. Throughout the pipeline, we record training and inference times at the model stages to quantify CPU-only latency and to assess the feasibility of deploying the resulting models on resource-constrained IoMT gateways.

4. RESULTS AND ANALYSIS

4.1 Experimental setup

We evaluate a two-stage pipeline on CICIoMT2024: Stage-1 (binary Normal vs Attack) and Stage-2 (14-class). Features are reduced via WOA; models are XGBoost and LightGBM with/without WOA. Metrics: Accuracy for Stage-1; Macro-/Weighted-F1 and per-class F1 for Stage-2.

Stage-1: Binary detection

Detection is near-perfect. WOA cuts dimensionality and training time with negligible accuracy loss; latency is CPU-friendly (summary in Table 6).

Table 6. Stage-1 binary detection — summary

Dataset/Model	Feats	Accuracy	Macro-F1	Train (s)	Infer (s)
Wi-Fi/MQTT — XGB	45	0.9975	0.9986	291.8	2.29
Wi-Fi/MQTT — WOA+XGB	18	0.9957	0.9976	91.9	1.25
Wi-Fi/MQTT — LGBM	45	0.9976	0.9987	77.4	3.81
Wi-Fi/MQTT — WOA+LGBM	18	0.9958	0.9976	55.4	3.17
BLE — LGBM	21	0.9991	0.9991	1.03	0.43
BLE — WOA+LGBM	12	0.9986	0.9986	0.61	—

Stage-2: Multi-class classification

Per-class Precision/Recall/F1 follows scikit-learn. WOA+XGBoost is high and stable (≈ 0.90–1.00) with a modest dip at UDP, while WOA+LightGBM varies more with lows at Ping_Sweep (~0.55) and VulScan (~0.35–0.40). See Figure 1 (per-class F1) and Figure 2 (confusion matrices), and the overall summary in Table 7.

Table 7. Stage-2 overall — macro/weighted-F1

Model	Accuracy	Macro-F1	Weighted-F1
WOA+XGBoost	0.9976	0.9599	0.9977
WOA+LightGBM	0.9864	0.8297	0.9859

Ablation on WOA

WOA prunes 40–60% features; training time drops 28–68% with minimal changes in accuracy/F1 (Table 8).

Table 8. WOA ablation — ΔDim and runtime

Slice/Model	Feats (Base→WOA)	ΔDim	ΔTrain	ΔInfer
Wi-Fi & MQTT — XGB	45→18	−60%	−68%	−45%
Wi-Fi & MQTT — LGBM	45→18	−60%	−28%	−17%
BLE — LGBM	21→12	−43%	—	—

BLE subset summary

On BLE, WOA preserves ≈ 0.999 accuracy while reducing detection time; see Table 9.

Table 9. BLE summary

Model	Feats	Accuracy	Macro-F1	Detect (s)
LGBM	21	0.9991	0.9991	1.03
WOA+LGBM	12	0.9986	0.9986	0.61

4.2 Deployment, limitations, and summary

From a deployment perspective, the proposed pipeline is designed to operate in real time under CPU-only constraints. All experiments were executed on a desktop-class processor (AMD Ryzen-class CPU with 12 cores and 64 GB RAM), while inference was intentionally restricted to a single core to emulate an IoMT edge gateway. The trained XGBoost and LightGBM models occupy only a few megabytes each and require less than a few hundred megabytes of RAM during inference, which is compatible with typical industrial and healthcare gateways equipped with 4–8 GB of RAM.

In terms of latency, the XGBoost binary detector processes approximately 1.05 million Wi-Fi/MQTT flows in about 2.29 s, corresponding to an average of roughly 2 µs per flow; the WOA-reduced variant further lowers this to approximately 1–1.2 µs per flow. Similar low per-sample latencies are observed for the BLE subset, indicating that the proposed pipeline can sustain real-time monitoring rates typical of hospital IoMT networks. Batching and lightweight quantization can further reduce inference latency if needed.

Despite these encouraging results, some limitations remain. Rare attack classes (e.g., VulScan and other low-frequency scans) are still challenging, particularly for LightGBM, which shows degraded F1-scores under extreme class imbalance. Potential remedies include class-balanced reweighting, focal loss, and hierarchical classification schemes that first separate broad attack families before distinguishing fine-grained subtypes.

In summary, WOA removes approximately 40–60% of the original features and reduces training time by up to 68% with minimal loss in detection accuracy. Across all experiments, XGBoost provides more stable per-class F1-scores than LightGBM, especially for minority classes, while LightGBM remains attractive when prioritizing speed. These trade-offs are illustrated in Figures 1 and 2 and Tables 6 and 8, and they highlight the practicality of combining WOA-based feature reduction with boosting models for IoMT intrusion detection

5. DISCUSSION

The study demonstrates that WOA-based feature selection significantly reduces dimensionality while preserving detection accuracy. By pruning 60% of features in the Wi-

Fi/MQTT slice, training and inference times dropped by more than half, with no statistically significant loss in AUC or F1. This confirms that redundant attributes in CICIoMT2024 can be safely removed, supporting the deployment of lighter IDS pipelines in constrained IoMT environments.

A key finding is the contrast between XGBoost and LightGBM. While both models achieved near-perfect binary detection, XGBoost showed superior multi-class stability (Macro-F1 ≈ 0.96) compared to LightGBM (Macro-F1 ≈ 0.83), especially for minority classes such as VulScan. BLE results were less challenging, reflecting the dominance of a single DoS attack, but the Wi-Fi/MQTT subset highlighted the benefits of WOA in managing heterogeneity and imbalance. Despite these improvements, minority classes remain problematic, echoing prior work on CICIoMT2024. Additional strategies such as hierarchical classification, data augmentation, or graph-based modeling may be required to close this gap. From a practical standpoint, the reduced inference latency (< 10 ms per packet window) and halved memory footprint indicate that the WOA+XGBoost pipeline is deployable on edge gateways in real healthcare networks.

6. CONCLUSION AND FUTURE WORK

This paper presented a WOA-augmented intrusion detection framework evaluated on the multi-protocol CICIoMT2024 dataset. The findings confirm that WOA can eliminate up to 60% of redundant features while sustaining near-perfect accuracy and AUC. XGBoost consistently outperformed LightGBM in multi-class settings, achieving a macro-F1 of 0.96 and demonstrating greater robustness on minority classes. BLE traffic, dominated by a single attack type, was comparatively easier to detect, whereas the heterogeneous Wi-Fi/MQTT slice highlighted the importance of feature reduction for both efficiency and fairness across classes. The reduced inference latency and halved memory footprint underline the practicality of deploying WOA-pruned models on IoMT edge gateways.

Despite these strengths, challenges remain. Minority attack types such as VulScan continue to exhibit low F1-scores, suggesting that boosting methods alone cannot fully address extreme imbalance. Furthermore, the computational cost of multi-class training remains significant.

Future research should explore: (i) hybrid schemes combining WOA with other metaheuristics to improve convergence dynamics, (ii) integration of graph neural networks or attention-based architectures to capture device-level and temporal dependencies, (iii) hierarchical and data augmentation approaches to enhance rare-class detection, and (iv) cross-dataset validation on BoT-IoT, ToN-IoT, and real hospital traces to strengthen generalizability. Together, these directions may lead to scalable, explainable, and resilient IDS solutions tailored for next-generation IoMT environments.

REFERENCES

[1] Canadian Institute for Cybersecurity. (2024). CICIoMT2024 dataset. University of New Brunswick. https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.

[2] Ramesh, K., Miller, N.C., Faridi, A., Aloul, F., Zualkernan, I., Sajun, A.R. (2024). Efficient machine learning frameworks for strengthening cybersecurity in internet of medical things (IoMT) ecosystems. In 2024 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, pp. 92-98. https://doi.org/10.1109/IoTaIS64014.2024.10799438

[3] Naeem, H., Alsirhani, A., Alserhani, F., Ullah, F., Krejcar, O. (2024). Augmenting Internet of Medical Things security: Deep ensemble integration and methodological fusion. Computer Modeling in Engineering Sciences, 141(3): 2185-2223. https://doi.org/10.32604/cmes.2024.056308

[4] Sánchez, N., Calvo, A., Escuder, S., Escrig, J., Domenech, J., Ortiz, N., Mhiri, S. (2024). Towards enhanced IoT security: Advanced anomaly detection using transformer models. In The 4th Workshop on Artificial Intelligence-Enabled Cybersecurity Analytics, Barcelona, Spain.

[5] Ayad, A.G., Sakr, N.A., Hikal, N.A. (2024) A hybrid approach for efficient feature selection in anomaly intrusion detection for IoT networks. The Journal of Supercomputing, 80(19): 26942-26984. https://doi.org/10.1007/s11227-024-06409-x

[6] Zhao, X., Li, D., Yang, B., Chen, H., Yang, X., Yu, C., Liu, S. (2015). A two-stage feature selection method with its application. Computers & Electrical Engineering, 47: 114-125. https://doi.org/10.1016/j.compeleceng.2015.08.011

[7] Shan, L. (2025). IoT network intrusion detection system using optimization algorithms. Scientific Reports, 15(1): 21706. https://doi.org/10.1038/s41598-025-04638-5

[8] AL-Husseini, H., Hosseini, M.M., Yousofi, A., Alazzawi, M.A. (2024). Whale optimization algorithm-enhanced long short-term memory classifier with novel wrapped feature selection for intrusion detection. Journal of Sensor and Actuator Networks, 13(6): 73. https://doi.org/10.3390/jsan13060073

[9] Adewole, K.S., Jacobsson, A., Davidsson, P. (2025). Intrusion detection framework for Internet of Things with rule induction for model explanation. Sensors, 25(6): 1845. https://doi.org/10.3390/s25061845

[10] Hafid, A., Rahouti, M., Aledhari, M. (2025). Optimizing intrusion detection in IoMT Networks through interpretable and cost-aware machine learning. Mathematics, 13(10): 1574. https://doi.org/10.3390/math13101574

[11] Dinh, P.V., Nguyen, D.N., Hoang, D.T., Nguyen, Q.U., Dutkiewicz, E., Bao, S.P. (2024). Multiple-input auto-encoder guided feature selection for IoT intrusion detection systems. arXiv preprint arXiv:2403.15511. https://doi.org/10.48550/arXiv.2403.15511

[12] Jouhari, M., Benaddi, H., Ibrahimi, K. (2024). Efficient intrusion detection: Combining x 2 feature selection with CNN-BiLSTM on the UNSW-NB15 dataset. In 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM), Leeds, United Kingdom, pp. 1-6. https://doi.org/10.1109/WINCOM62286.2024.10658099

[13] Ghubaish, A., Yang, Z., Erbad, A., Jain, R. (2023). LEMDA: A novel feature engineering method for intrusion detection in IoT systems. IEEE Internet of Things Journal, 11(8): 13247-13256. https://doi.org/10.1109/JIOT.2023.3328795

[14] Mutleg, M.L., Mahmood, A.M., Al-Nayar, M.M.J.

(2024). A comprehensive review of cyber-attacks targeting IoT systems and their security measures. International Journal of Safety & Security Engineering, 14(4): 1073-1086. https://doi.org/10.18280/ijsse.140406
[15] Mutleg, M.L., Mahmood, A.M., Jawad Al-Nayar, M.M. (2024). Deep learning based intrusion detection system of IoT technology: Accuracy versus computational complexity. International Journal of Safety & Security Engineering, 14(5): 1547-1558. https://doi.org/10.18280/ijsse.140522
[16] Altameemi, A.I., Mohammed, S.J., Mohammed, Z.Q., Kadhim, Q.K., Ahmed, S.T. (2024). Enhanced SVM and RNN classifier for cyberattacks detection in underwater wireless sensor networks. International Journal of Safety & Security Engineering, 14(5): 1409-1417. https://doi.org/10.18280/ijsse.140508
[17] Al-Ameer, A., Asraa, A., Bhaya, W.S. (2023). Intelligent intrusion detection based on multi-model federated learning for software defined network. International Journal of Safety & Security Engineering, 13(6): 1135-1141. https://doi.org/10.18280/ijsse.130617
[18] Xue, B., Zhang, M., Browne, W.N., Yao, X. (2015). A survey on evolutionary computation approaches to feature selection. IEEE Transactions on Evolutionary Computation, 20(4): 606-626. https://doi.org/10.1109/TEVC.2015.2504420
[19] Mafarja, M., Mirjalili, S. (2018). Whale optimization approaches for wrapper feature selection. Applied Soft Computing, 62: 441-453. https://doi.org/10.1016/j.asoc.2017.11.006
[20] Tawhid, M.A., Ibrahim, A.M. (2020). Feature selection based on rough set approach, wrapper approach, and binary whale optimization algorithm. International Journal of Machine Learning and Cybernetics, 11(3): 573-602. https://doi.org/10.1007/s13042-019-00996-5
[21] Chandrashekar, G., Sahin, F. (2014). A survey on feature selection methods. Computers & Electrical Engineering, 40(1): 16-28. https://doi.org/10.1016/j.compeleceng.2013.11.024