Efficient Hybrid Machine Learning and Feature Selection Approach for IoMT Attack Detection and Healthcare Security Enhancement

Mustafa Hasan Merza
Arts, Sciences & Technology University in Lebanon, Lebanon
Email: mustafamerza.eng@gmail.com

Article History

Received: Nov. 11, 2025
Revised: Feb 07, 2026
Accepted: Feb 12, 2026

Abstract

The increasing interconnectivity of healthcare devices through the Internet of Medical Things (IoMT) has improved patient monitoring and treatment, but also exposed these systems to malicious cyberattacks that threaten both patient safety and data integrity. Existing machine learning (ML)-based approaches have attempted to detect such attacks, but most rely on all dataset features, including irrelevant and redundant ones, which increases computational cost and reduces detection accuracy. Feature selection techniques such as Particle Swarm Optimization (PSO) have been used to address this challenge, yet their default fitness functions fail to select the most suitable features for each classifier, often leading to suboptimal results. To overcome these limitations, this study introduces a novel fitness function integrated with PSO and ML classifiers to identify the most relevant features for accurate attack detection in IoMT devices. The proposed framework was evaluated using the NSL-KDD dataset (41 features) with RF, KNN, SVM, and LR classifiers. The number of correctly predicted labels for the optimal feature subsets was 99.35% for RF, 99.02% for KNN, 98.20% for SVM, and 97.61% for LR, whereas the baseline accuracies for the cases with all the features were 95.41%, 94.76%, 92.86%, and 89.55%, respectively. Moreover, the execution times decreased by almost one-third, showing the efficiency of the method. The report indicates validation of the PSO-based fitness function developed for lightweight-accuracy attacks detection in IoMT devices, thus proving to be efficient and cost-conducive, readily deployable in medical organizations as well as smart home environments, thereby safeguarding future-proof healthcare infrastructures against dynamically evolving threats.

Keywords- Internet of Medical Things (IoMT), Intrusion Detection System (IDS), Particle Swarm Optimization (PSO), Machine Learning (ML), Cybersecurity, Smart Healthcare, Attack Detection.

I. INTRODUCTION

The Internet of Medical Things is a binary interface that connects medical devices and wearables to computerized platforms [1]. Through this digital connection, one can carry out real-time monitoring of patients and make rapid decisions about clinical care through personalized pathways and interventions early in medical care. Continuous collection of data indicates the capacity of patient management provided through connected devices such as wearable health trackers, smart infusion systems, and linked diagnosis mechanisms. The IoMT promises strategic cost reductions in the treatment of patients, efficiency gains in service provision, and generally wider access to medical facilities, in addition to improving patient care. Collectively, these capabilities highlight the transformative potential of IoMT in modern healthcare delivery. [2], [3]. AI or Artificial Intelligence, and particularly ML, which is shorthand for Machine Learning, is now a powerful tool in a lot of domains because it can automatically learn patterns in data and predict very accurately [4]. The ML algorithms control all the aspects of intelligent transport systems, from the detection of vehicles to traffic monitoring, and the possible performance of safe and efficient management of roads [5]. According to computer vision [6], artificial intelligence does utilize important techniques, such as machine learning, for object detection, image classification, and scene analysis, building up applications such as autonomous driving, surveillance, and human-computer interaction. Health is where currently ML-based algorithms have been proven to be productive in developing applications, such as disease identification, and the analysis of medical signals, where they are capable of high accuracy in identifying pathological conditions in physiological signals [6]. For instance, applications of machine learning in terms of classifying electroencephalography (EEG) signals have been indicated to be particularly useful for the detection of neurological disorders while employing electrocardiogram signals for research on the detection of arrhythmia and cardiac conditions [7, 8]. One can see the performance gap in such examples between ML and other methods

because of how much better ML-driven solutions usually are in accuracy, scalability, and adaptability-all indispensable properties of AI which open new horizons in innovative medical-to-technological conjunctions.

These past few years have seen the machine learning (ML) techniques being put to use in various applications in identifying cyberattacks directed at the IoMT devices. But among the most effective is an IDS that is all-embracing in using all features supplied in such a benchmark dataset, most of which are unnecessary or redundant because of the computational expense involved and also lower accuracy in classification. The best means of addressing all these problems is through the implementation of feature selection techniques based on the metaheuristic method, which commonly uses PSO as the way to go, or other methods. However, they generally make use of default fitness functions, which tend to overlook the selection of the most suitable features based on each classifier, resulting mostly in poorer outputs or accuracy, as [9, 10] pointed out. Thus, in the present study, a new fitness function will be introduced that is combined with PSO and ML classifiers for optimizing the selection of features in intrusion detection in IoMT environments. In this way, the proposed framework guarantees that every classifier will be trained using an optimized subset of features, hence increasing accuracy and efficiency. Here lie the crucial contributions of this study:

- Development of an efficient fitness function integrated with PSO and ML classifiers to improve attack detection performance in IoMT environments.
- Demonstration of accuracy improvements for all classifiers, where RF, KNN, SVM, and LR achieved 99.35%, 99.02%, 98.20%, and 97.61%, respectively, compared to their baseline accuracies of 95.41%, 94.76%, 92.86%, and 89.55% when all features were used.
- Analysis of the execution time, where PSO-based feature selection reduced runtime by up to 35%, making the proposed framework lightweight and practical for real-world deployment in medical organizations and smart home environments for IoMT attack detection.

II. RELATED WORKS

Several studies have explored intrusion detection in IoMT using machine learning and deep learning approaches to improve security against evolving threats. The key related studies reviewed in this section closely follow the datasets that are quite popular, and then the methodology, findings, and limitations in reviewing these related works. For example, Avula and Bachala [11] introduced a SIDHELNet, a specific intrusion detection framework for IoMT environments. This model uses parallel Bi-LSTM and Bi-GRU layers using Word2Vec semantic embeddings to produce an enriched temporal-spatial representation of network traffic, which is then passed through a nine-classifier heterogeneous ensemble. SIDHELNet proved its worth in intrusion detection with an astounding 99.61% detection accuracy and precision, recall, and F1-score all greater than 99.5%. This clearly shows the framework's capacity to detect complex intrusion patterns in traffic streams in IoMT. However, the high dependence on deep architectures and classifiers might create computational overhead for deployment in resource-constrained IoMT devices.

To make IoMT networks more resilient against data quality and class imbalance challenges, Salehpour et al. [12] have proposed a hybrid intrusion detection framework. The proposed framework comprises three major modules: an XGBoost-based noise detection model for filtering anomalous records, ADASYN-based adaptive resampling to balance skewed classes, and a Random Forest classifier for final intrusion detection. The model was thoroughly evaluated using the UNSW-NB15 dataset, achieving a detection accuracy of 92.23%, thus proving its robustness against noise and class imbalance. Noise and imbalance are addressed through preprocessing and augmentation. This suggests that data quality plays a very important role in IDS performance. Still, the pre-processing steps are highly computationally intensive, and the number of datasets tested may not be sufficient for scaling to large-scale real-time IoMT environments. Farhan et al. [13] also proposed a Residual Network-based Convolutional Neural Network (ResNet-CNN) to resolve weaknesses of traditional IDS for detecting heterogeneous and evolving cyberattacks. Unlike conventional models relying on manual feature engineering, the proposed one uses deep residual connections with CNN layers to automatically extract strong representations of network traffic. The framework was thoroughly tested across numerous experimental setups on the NSL-KDD dataset, such as binary, multiclass, and feature division-based classifications. The model inflated its accuracy up to 98.94 and 98.92% accurate for binary and multiclass classification, respectively, while each of the individual attack types exceeded 99% accuracy. It brings to light the power of residual connections to increase generalization and robustness, but this study is still limited to only one dataset (NSL-KDD), which requires further validation on more complicated benchmarks, such as UNSW-NB15, to test its flexibility in real-world IoMT intrusion scenarios.

With the increasing cybersecurity threat to patient safety and data integrity, Goumidi and Pierre developed a framework for real-time anomaly detection in Internet of Medical Things (IoMT) systems. To overcome the unavailability of healthcare-specific benchmarks, they developed a novel medical dataset from the UNSW-NB15 dataset and supplemented it with relevant attack types such as data falsification and denial-of-service (DoS). The dataset has more than 250,000 records with a challenging 60% anomaly ratio to capture a realistic test environment. The authors conducted seven machine learning algorithms, followed by proposing a stacking ensemble model consisting of Random Forest and ANN as base learners with XGBoost as the meta-learner. The system accuracy of 98.02% on the medical dataset was also promising for it on the UNSW-NB15 benchmarked dataset. However, despite those improvements, the study only reached moderate performance vis-a-vis contemporary IDS approaches, which emphasizes the need for further refinements and wider validations across various traffic types of IoMT. Khan et al. [15] proposed an MLP-based intrusion detection framework for IoMT-based smart healthcare systems to protect the SHS from malicious attacks. It implements deep learning for automatic feature learning, optimizing performance on both NSL-KDD and UNSW-NB15 benchmark datasets. The experimental results showed that the

developed IDS recorded 95.06% accuracy, significantly surpassing other comparable deep learning techniques, yet associated with lower false positive rates. These results prove the feasibility of MLP architectures in the detection of threats in health networks. Also, the study was limited to supervised learning on static datasets, which rendered it inflexible towards evolving and zero-day attack scenarios. This calls for increased enhancement in flexibility and robustness through instilling advanced learning or feature selection schemes capable of addressing unseen attack patterns and also incorporating real-time IoMT telemetry to strengthen detection under dynamic conditions.

The study referred to in [16] aimed to find out how feature selection and normalization techniques affect the functioning of AI-based intrusion detection systems (IDS) and backed the assessment with different benchmark datasets. In addition, a decision tree wrapper-based approach to feature selection using min-max normalization was proposed to improve model efficiency. With different algorithms tested on the NSL-KDD and UNSW-NB15 datasets, Random Forest (RF) was always the winner on all counts. For example, RF achieved an accuracy of 99.86% in the NSL-KDD case, with great detection accuracy resulting from wrapper-based feature selection. This result points to the necessity of stringent preprocessing schemes that would optimize the performance of the IDS systems, especially in the cases of larger and more complex datasets. However, the framework was found to be dataset-dependent and less adaptable; results were greatly varied across the datasets, and the evaluation did not cover real-time IoMT scenarios. Hence, it indicates the need to enhance generalization, adaptability, and resilience in a continuously changing IoMT traffic condition. In [17], an advanced IDS framework is presented based on ResNet-BiGRU with an attention mechanism, where ResNet extracts local traffic features and BiGRU captures long-term dependencies, while attention assigns weights to the most relevant features. To further improve model generalization, the hyperparameters were automatically tuned using a PSO–GA hybrid optimization strategy, which dynamically adjusted particle swarm parameters and applied genetic mutation to escape local optima. The approach was evaluated on multiple benchmark datasets, including UNSW-NB15, where it achieved an accuracy of 95.17%. Although the method demonstrated strong detection capability, the results on UNSW-NB15 reflected only moderate accuracy compared to state-of-the-art IDS models, indicating limited effectiveness in handling the complexity of modern IoMT traffic. A comparative summary of the reviewed IoMT intrusion detection studies, including their methods, datasets, best results, strengths, and limitations, is presented in Table I.

TABLE I. SUMMARY OF RELATED WORKS ON IOMT INTRUSION DETECTION.

Study	Proposed Method	Dataset	Best Accuracy	Strengths	Limitations
Avula & Bachala [11]	SIDHELNet (Word2Vec + BiLSTM + BiGRU + Heterogeneous Ensemble)	UNSW-NB15	99.61%	Robust ensemble with strong adaptability	High computational complexity, limited suitability for resource-constrained IoMT devices
Salehpour et al. [12]	Hybrid IDS (XGBoost Noise Detection + ADASYN + Random Forest)	UNSW-NB15	92.23%	Effective noise handling and imbalance correction	Computationally expensive preprocessing, limited scalability
Farhan et al. [13]	ResNet-CNN	NSL-KDD	98.94% (binary), 98.92% (multiclass)	Strong automatic feature extraction	Evaluated only on NSL-KDD, lacks generalization to newer datasets
Goumidi & Pierre [14]	Stacking Ensemble (RF + ANN, XGBoost meta-learner)	UNSW-NB15, Medical Dataset	98.02%	Real-time validation, healthcare-relevant attack simulation	Moderate accuracy vs. SOTA, limited attack diversity
Khan et al. [15]	MLP-based IDS	NSL-KDD, UNSW-NB15	95.06%	Low false positive rate, simple deep model	Moderate accuracy, supervised-only, lacks adaptability to zero-day attacks
Umar et al. [16]	Wrapper-based Feature Selection + RF	NSL-KDD, UNSW-NB15	99.86% (NSL-KDD), 96.01% (UNSW-NB15)	Preprocessing boosts IDS performance, strong RF results	Dataset-dependent, no IoMT-specific real-time evaluation
Xia et al. [17]	ResNet-BiGRU + Attention + PSO-GA Hyperparameter Optimization	UNSW-NB15	95.17%	Automated hyperparameter tuning, improved generalization	Lower accuracy on UNSW-NB15, limited IoMT adaptability

III. PROPOSED METHODOLOGY

The proposed framework for IoMT intrusion detection follows a structured pipeline, as illustrated in Figure 1. The process begins with dataset preparation, where IoMT traffic data is divided into training and testing sets. The training data undergoes a preprocessing stage using Min–Max normalization to standardize feature values. The classifiers RF, SVM, LR, and KNN are tested using Accuracy, Precision, Recall, and F1-score, with the confusion matrix providing a more detailed interpretation of the results. Before this stage, PSO is used to choose the most useful features, creating a reduced subset that enhances the efficiency and accuracy of the training process.

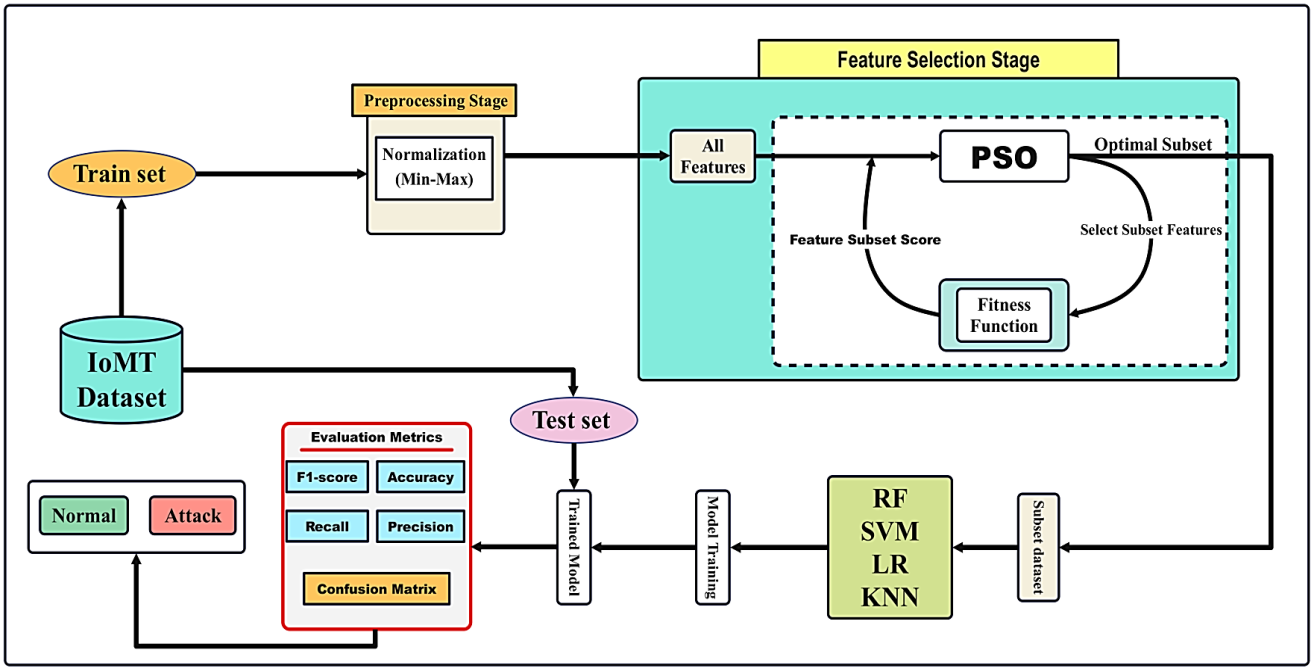

Figure 1: Workflow of the proposed IoMT intrusion detection framework.

A. IoMT dataset description

Evaluating an intrusion detection system for IoMT requires diverse and reliable datasets that represent both traditional and modern attack behaviors. To ensure a fair assessment, this study makes use of a popular benchmark dataset: NSL-KDD [18]. The NSL-KDD dataset was first considered because it provides a balanced and cleaned version of the earlier KDD'99 dataset. It contains 148,517 instances divided into 22,544 testing samples and 125,973 training samples, distributed across 41 features. The dataset defines five main attack categories, making it suitable for evaluating baseline IDS models in healthcare-related applications. Its reduced redundancy compared to KDD'99 makes it a reliable benchmark for testing classification algorithms. By employing both datasets, the proposed IDS can be evaluated across different levels of difficulty: NSL-KDD represents a classic but balanced benchmark. This dataset strategy ensures improved generalization and helps reduce bias that may occur when relying on a single dataset. A comparison of the main dataset characteristics is provided in Table II.

TABLE II. OVERVIEW OF THE BENCHMARK DATASET USED FOR IOMT INTRUSION DETECTION.

Name of Dataset	Attack Categories	Features	Total Records	Training Samples	Testing Samples
NSL-KDD	5	41	148,517	125,973	22,544

B. Pre-processing IoMT Dataset Using Min–Max Normalization

Before training the proposed IDS, the raw data from both datasets must be standardized to ensure fair contribution of all features. Network traffic attributes in IoMT datasets often vary widely in scale; for example, some features represent simple binary values, while others capture continuous values with very large ranges [19, 20]. If left unprocessed, features with higher magnitudes could disproportionately influence the classifier, reducing overall detection performance. Min-Max normalization solved this problem as a preprocessing technique. The mathematics of Min-Max transformation rescales each feature so that it lies in a fixed range of values from 0 to 1; hence, it makes all features uniformly influential over the dataset [21]. The transformation is calculated using the following formula:

$$A = \frac{B - min(fe)}{max(fe) - min(fe)} \quad (1)$$

where: B is the original value, A is the normalized value, $max(fe)$ and $min(fe)$ are the minimum and maximum values of the feature vector. The scaling used aids accelerated convergence of learning algorithms with added assurance of performance reliability. Normalization further aids in diminishing training-induced bias and enables the models to pick up on subtle anomalies in IoMT traffic. This preprocessing step thus provides a stable ground for subsequent stages of feature selection and classification.

C. Feature Selection using PSO Method

IoMT intrusion detection, datasets typically include a large number of attributes, many of which may not be equally useful for identifying attacks. The presence of irrelevant or redundant features increases computational cost, slows down processing, and can even reduce detection accuracy [22, 23]. To overcome these issues, this work integrates a feature selection stage to retain only the most informative attributes before classification. Among different feature selection techniques, PSO is adopted due to its efficiency and adaptability. PSO is a population-based optimization algorithm inspired by the cooperative movement of bird flocks. In this approach, each potential feature subset is treated as a particle, and the swarm collectively explores the search space to find an optimal combination of attributes [24, 25]. The selection process is guided by both the experience of individual particles (personal best) and the performance of the swarm as a whole (global best). These two factors influence the position and velocity adjustments of each particle during the process of optimization, keeping a balance between exploration (searching for novel feature subsets) and exploitation (refining selected promising subsets). The update process is formally expressed as:

$$\boldsymbol{v_i^{(t+1)}} = S\, v_i^{(t)} + Q_1\, M_1(p_i^{best} - x_i^{(t)}) + Q_2\, M_2\, (g^{best} - x_i^{(t)}) \qquad (2)$$

$$\boldsymbol{x_i^{(t+1)}} = \boldsymbol{x_i^{(t)}} + \boldsymbol{v_i^{(t+1)}} \qquad (3)$$

where $\boldsymbol{x_i^{(t)}}$ and $v_i^{(t)}$ denote the position and velocity of particle pbest is its best-known position, and gbest is the best solution discovered by the swarm. Feature selection in PSO is initiated by encoding potential solutions as binary strings, with individual bits indicating whether a feature is retained (1) or discarded (0). To evaluate the quality of a particle, a novel fitness function F is designed that jointly considers classification accuracy, dimensionality reduction, and stability of the classifier across folds. The function is given as:

$$\mathrm{F} = \alpha \cdot (1 - \mathrm{Accuracy}) + \beta \cdot \frac{Selected\ Features}{\mathrm{Total\ Features}} + \gamma \cdot \mathrm{Variance(Accuracy)} \quad (4)$$

Through PSO, the input dataset is first streamlined by a process of dimensionality reduction, subsequent removal of residual features, and only those features that are most informative are retained. This mechanism yields compact, accurate, and consistent feature subsets across validation trials. Hence, detection performance is improved, with reduced computational overhead, thereby enabling the IDS to function efficiently on resource-constrained IoMT devices.

D. Classification models

The proposed IDS underwent empirical evaluation by deploying four very well-known machine learning tools, namely, RF, KNN, LR, and SVM. Their complementary characteristics provided a great basis for comparison of the classification results in the IoMT environment.

- RF is an ensemble learning algorithm that constructs multiple decision trees during training and combines their outputs through majority voting. Its robustness against overfitting and ability to handle high-dimensional data make it suitable for detecting diverse IoMT intrusion patterns [26].
- KNN is a classification method that assigns a label to a sample based on the majority class among its nearest neighbors. KNN is simple and effective for pattern recognition in IoMT traffic, but its performance can be affected by noisy features and large datasets without prior feature selection [27].
- LR is a statistical model that estimates the probability of a data instance belonging to a specific class using a logistic function. Despite its simplicity, LR provides strong baseline performance and interpretable decision boundaries, which are valuable in the healthcare domain for intrusion detection transparency [28].

SVM seeks to find an optimal hyperplane that maximizes the margin between classes. By applying kernel functions, SVM can effectively handle non-linear separations in IoMT traffic data. Its strength lies in high accuracy with well-separated data, though it may require high computational resources for large datasets [29].

E. Evaluation Metrics

Evaluating an intrusion detection system in the IoMT domain requires reliable metrics that can measure not only overall accuracy but also the balance between detecting attacks and avoiding false alarms. Since IoMT traffic includes both normal medical data and malicious attack patterns, four standard performance indicators are applied: Accuracy, Precision, Recall, and F1-score.

- Accuracy: is defined as the ratio between the total number of correctly predicted samples, covering both normal and attack classes, and the overall number of samples in the dataset [30]:

$$\text{Accuracy} = \frac{TP+TN}{TN+TP+FN+FP} \quad (5)$$

- Precision: measures the proportion of instances identified as attacks that are truly attacks [31]:

$$\text{Precision} = \frac{TP}{TP+FP} \quad (6)$$

- Recall: measures the ability of the model to identify actual attacks among all malicious traffic, ensuring that harmful activities are not overlooked [32]:

$$\text{Recall} = \frac{TP}{TP+FN} \quad (7)$$

- F1-score: provides a balanced metric by combining Precision and Recall through their harmonic mean [33]:

$$\text{F1} - \text{score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Recall} + \text{Precision}} \quad (8)$$

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The effectiveness of the proposed IoMT intrusion detection framework was examined under two experimental conditions. In the first condition, the four machine learning classifiers (RF, LR, KNN, and SVM) were tested on two datasets using all available features, without applying feature selection. In the second condition, the same classifiers were evaluated after applying PSO-based feature selection, where only the most relevant attributes were retained. This setup allows a direct comparison between the baseline models and the optimized models, highlighting the role of PSO in improving detection accuracy and efficiency. The hyperparameters used for PSO and the machine learning models are summarized in Table III.

TABLE III. KEY HYPERPARAMETERS OF CLASSIFIERS AND PSO USED IN THE WORK.

Method	Hyperparameters
PSO	Swarm size = 40, inertia weight = 0.9, acceleration coefficients $c1$=$c2$=2, iterations = 100
RF	100 trees, max depth = 15
LR	Learning rate = 0.01, Max iterations = 1000
SVM	Kernel = Radial Basis Function (RBF), C=1.0
KNN	k=5, distance = Euclidean

A. Results of Models without Feature Selection using PSO

In the first experimental condition, the machine learning models were trained and tested using all available features from the benchmark dataset, namely 41 features from NSL-KDD. No feature reduction or optimization was applied in this stage. The metrics, involving Recall, Accuracy, F1-score, and Precision, are summarized in Table IV.

TABLE IV. EVALUATION OF CLASSIFIERS TRAINED WITH ALL 41 FEATURES.

ML Models	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
SVM	92.2	93.45	92.82	92.86
KNN	94.04	95.43	94.73	94.76
LR	89.73	89.46	89.6	89.55
RF	95.52	95.33	95.42	95.41

Compared with the other classifiers, RF provided the best accuracy of 95.41%. KNN achieved a slightly lower result of 94.76%, while Support Vector Machine obtained 92.86%. The lowest performance was recorded by LR with an accuracy of 89.55%. These findings highlight the strengths of ensemble-based and distance-based classifiers in handling high-dimensional intrusion detection data.

Specifically, RF benefits from aggregating multiple decision trees, which reduces overfitting and improves generalization, while KNN effectively captures local similarity patterns within the large feature space. On the other hand, LR struggled to separate attack and normal traffic when using the full feature set, which explains its relatively lower performance. Overall, the use of all features provided a baseline comparison, but the large number of attributes 41 in NSL-KDD may introduce redundancy, noise, and higher computational cost. After identifying this limitation, the process moved to a PSO feature selection stage, where the feature space was reduced to improve classification accuracy and speed.

B. Classification results of models with the most relevant features chosen by PSO

In the second experimental condition, PSO was applied to select the most relevant features from the NSL-KDD dataset, reducing the dimensionality from 41 original features to a smaller optimized subpart. The choices attributes were then used to train the four ML models. The results, measured in terms of Precision, Recall, F1-score, and Accuracy, are presented in Table V.

TABLE V. OVERVIEW OF THE BENCHMARK DATASET USED FOR IOMT INTRUSION DETECTION.

ML Models	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
SVM	98.46	97.97	98.21	98.2
KNN	98.67	99.37	99.02	99.02
LR	97.7	97.55	97.62	97.61
RF	**99.26**	**99.44**	**99.35**	**99.35**

The results show a significant improvement compared to the case where all 41 features were used. For example, among all classifiers, RF delivered the strongest results, reaching 99.35% accuracy, while KNN closely followed with 99.02%. Similarly, SVM and LR also recorded high accuracies of 98.20% and 97.61%, respectively. These findings clearly indicate that PSO-based feature selection enhances classifier performance by removing redundant and irrelevant attributes, enabling the models to concentrate on the most relevant features. The improvements are particularly noticeable in KNN and SVM, which are sensitive to noisy or high-dimensional data. Overall, PSO reduced computational complexity and boosted classification accuracy, making the framework more suitable for real-time IoMT intrusion detection.

C. Confusion Matrix Analysis after PSO-based Feature Selection for NSL-KDD dataset

The confusion matrices for the four classifiers after applying PSO-based feature selection are illustrated in Figure 2. Each matrix presents the distribution of correctly and incorrectly classified samples between Normal and Attack classes.

- SVM: Out of all samples, 3326 normal and 3289 attack instances were correctly classified, with only 121 misclassifications (52 false positives and 69 false negatives). This shows that SVM achieved a strong balance between detecting attacks and avoiding false alarms.
- KNN: KNN produced one of the best results, with 3333 normal and 3337 attack samples correctly classified, and only 66 misclassifications. The low number of false positives (45) and false negatives (21) reflects how PSO enhanced KNN's ability to handle noisy and redundant features.
- LR: LR achieved good results but had slightly more errors than other models, with 3300 normal and 3275 attack instances correctly classified. The presence of 78 false positives and 83 false negatives suggests that LR, being a linear model, struggled more with complex decision boundaries, though PSO still improved its performance in contrast to using all features.
- RF: RF demonstrated the best classification outcome, with 3353 normal and 3339 attack samples correctly identified, and only 44 misclassifications in total (25 false positives and 19 false negatives). The extremely low error rates highlight RF's strength in leveraging the optimized feature subset produced by PSO.

Overall, the confusion matrices confirm that PSO reduced classification errors across all models by eliminating irrelevant attributes and focusing on the most discriminative features. This improvement is especially noticeable in KNN and RF, which achieved near-perfect separation between normal and attack traffic. Such reliable detection is critical for securing IoMT environments, where minimizing false alarms while accurately identifying malicious activity is essential for patient safety and system reliability.

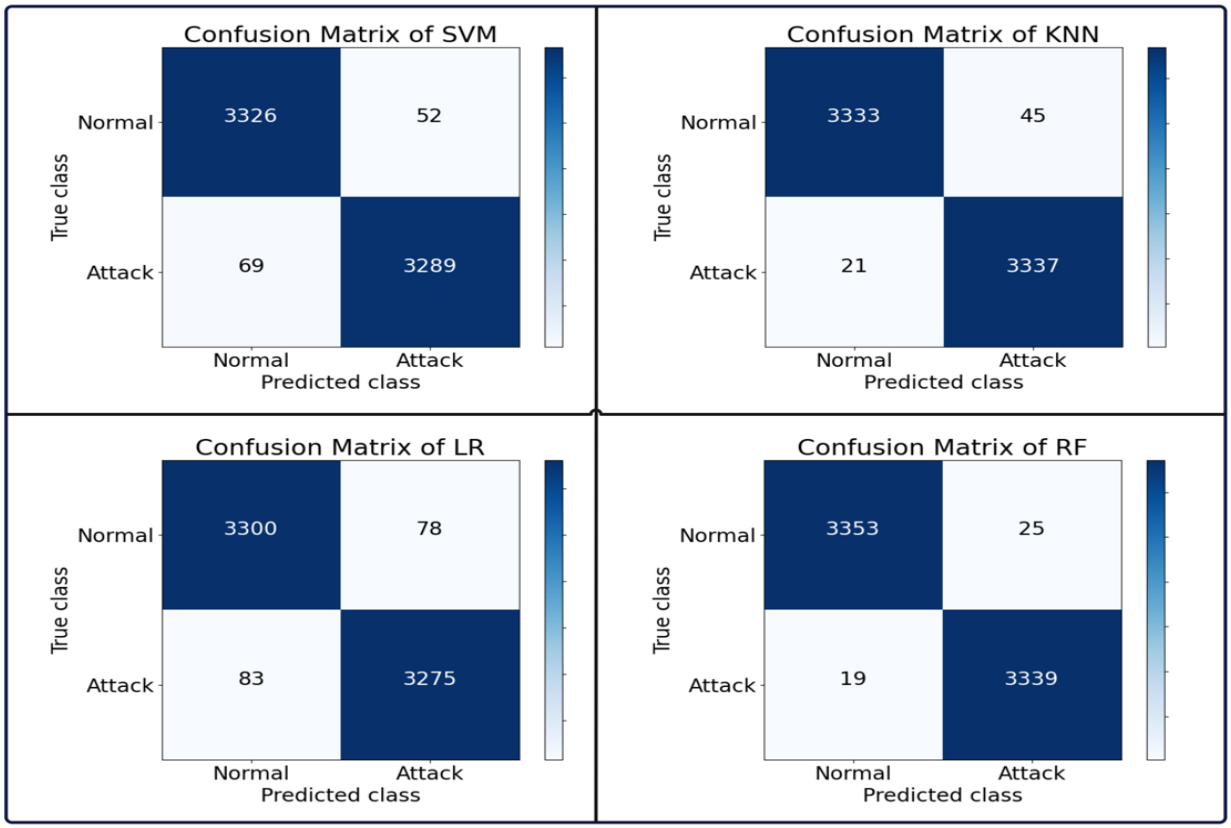

Figure 2: Confusion matrices showing the detection performance of four classifiers with PSO optimization.

Figure 3 presents a comparison of the four models' classification performance with the application of PSO-based feature selection. The confusion matrices highlight that the number of correctly classified samples increased for all classifiers after applying PSO. For example, RF improved from an accuracy of 95.41% (without PSO) to 99.35% (with PSO), while KNN rose from 94.76% to 99.02%. Similarly, SVM improved from 92.86% to 98.20%, and LR from 89.55% to 97.61%. These results confirm that PSO not only reduced misclassifications but also significantly enhanced the accuracy of all models.

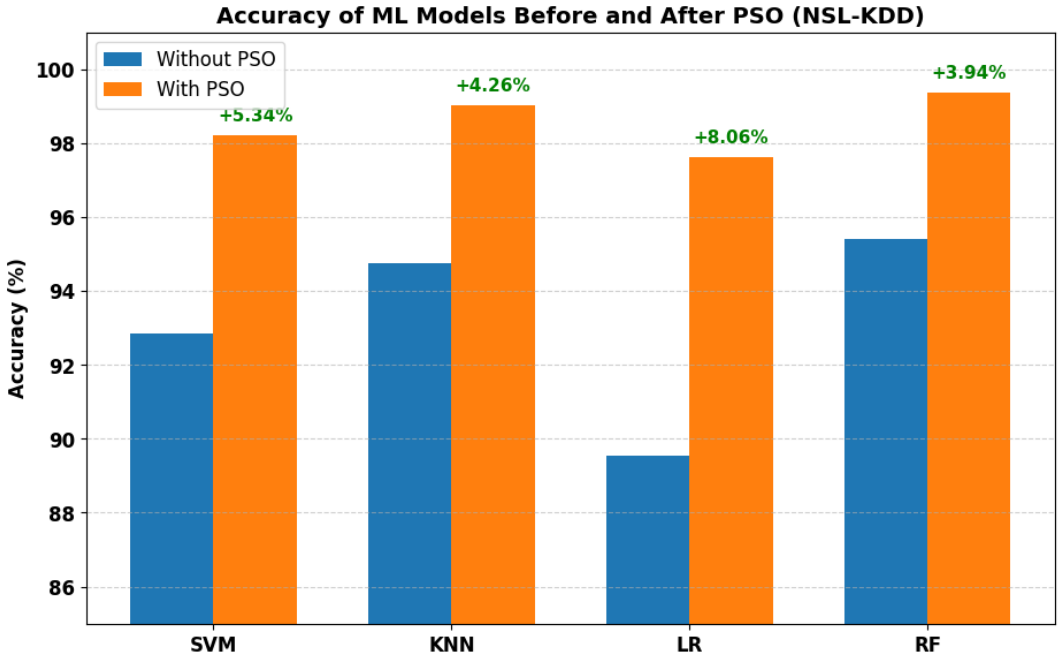

Figure 3: Accuracy improvement of SVM, KNN, LR, and RF using PSO-optimized features.

D. Execution Time Analysis

The testing and training times of KNN, RF, SVM, and LR were recorded under two scenarios: the full 41-feature NSL-KDD dataset and the reduced feature set obtained through PSO. This comparison highlights the importance of computational efficiency, which is essential in IoMT environments where systems face strict constraints on resources and latency alongside the need for high detection accuracy. The results, summarized in Table VI, show that execution time was consistently lower after PSO-based feature selection. This improvement is due to the reduction in feature dimensionality, which decreases the computational burden on classifiers during both training and inference. RF and KNN are those algorithms whose runtime were reduced the most, due to the very fact that they are highly sensitive to the input attributes; SVM and LR also experienced some decrease in runtime, but not to such a great degree as the former. The analysis shows that PSO enhances runtime efficiency while improving classification accuracy by eliminating the non-influential features. This dual benefit is crucial in IoMT applications, wherein real-time monitoring and rapid threat detection severely affect patient safety and system reliability.

TABLE VI. EXECUTION TIME OF CLASSIFIERS.

Classifier	Time without PSO (MS)	Time with PSO (ms)	Improvement (%)
RF	2.85	1.95	31.6%
KNN	3.42	2.21	35.4%
SVM	2.14	1.62	24.3%
LR	1.36	1.01	25.7%

E. Comparison with Recent Studies

Several recent efforts have worked on employing various techniques on the NSL-KDD dataset towards better intrusion detection in IoMT environments. For example, Farhan et al. [13] used the deep learning model ResNet-CNN, which has an accuracy of 98.92%, while Khan et al. [15] utilized an MLP-based IDS, which achieved an accuracy of 95.06%. This indicates that deep models are quite powerful, but the fact that they require more computational power may deter them from being utilized in real-time IoMT systems. Other works include the combination of feature selection with traditional machine learning classifiers. Similarly, study [34] applied PCA-PSO with SVM and reached 98.5% accuracy, confirming the importance of dimensionality reduction. Swarm-intelligence–based methods with deep models have also been explored. Study [36] developed an SSA-LSTM model, achieving 97.89% accuracy, but at the cost of higher training complexity due to deep recurrent structures. In comparison, the proposed PSO-based feature selection combined with RF, KNN, SVM, and LR reached a maximum accuracy of 99.35% on NSL-KDD. As shown in Table VII, the proposed system outperforms most related studies while maintaining lower complexity, making it highly suitable for resource-constrained IoMT applications.

TABLE VII. COMPARISON OF PROPOSED APPROACH WITH RECENT STUDIES.

Study	Method	Dataset	Accuracy (%)	Remarks
[13]	ResNet-CNN	NSL-KDD	98.92	Strong DL model, but resource-intensive
[15]	MLP-based IDS	NSL-KDD	95.06	Lower accuracy, simple supervised approach
[34]	PCA + PSO + SVM	NSL-KDD	98.50	Hybrid FS, good results but below our approach
[35]	RF + K-means + Cuckoo Search	NSL-KDD	98.7	Complex approach contains feature selection and clustering stages
[36]	SSA + LSTM	NSL-KDD	97.89	High complexity, lower accuracy
Proposed Approach	**Efficient fitness function for PSO-based FS + RF/KNN/SVM/LR**	**NSL-KDD**	**99.35**	**High accuracy with reduced features, efficient for IoMT**

V. CONCLUSION

This study introduces an efficient fitness function in Particle Swarm Optimization (PSO) for feature selection for intrusion detection in the Internet of Medical Things (IoMT) environments, using 41 features in the NSLKDD dataset. The main thrust of the study is to select the most relevant attributes in a bid to enhance classifier accuracy while minimizing computational overhead. The performance measures obtained from experiments demonstrate that the feature selection based on PSO enhanced performance considerably when compared with the use of all features. For training for all 41 features, the classifiers had the baseline accuracies of 95.41%(RF), 94.76%(KNN), 92.86%(SVM), and 89.55%(LR). After applying PSO, the accuracies increased to 99.35%(RF), 99.02%(KNN), 98.20%(SVM), and 97.61%(LR). These results emphasize that removal of irrelevant and redundant features increases efficiency and

accuracy of detection, with RF and KNN scoring the highest improvement. This, in turn, proves that PSO can serve effectively in taking away the guesswork for feature selection, applying in its path classical ML models that achieved performance levels comparable to their states-complex deep-learning counterparts but at greatly reduced computational cost. IoMT systems need real-time detection and efficient resource usage in order to work effectively, making this paradigm a good fit. Moreover, the PSO also reduced the features' dimensionality, thus aiding in improved accuracy based on faster convergence and lesser training complexity. Looking ahead, future research will focus on testing the framework on larger and more diverse IoMT datasets, integrating real-time device telemetry to support adaptive detection, exploring hybrid optimization strategies such as GWO, SSA, and WOA for improved resilience against zero-day attacks, and embedding explainable AI methods to increase interpretability in healthcare security applications.

ACKNOWLEDGMENT

This work was supported by the Arts, Sciences & Technology University in Lebanon and the College of Engineering, Al-Iraqia University.

REFERENCES

[1] D. V. Dimitrov, “Medical internet of things and big data in healthcare,” Healthcare informatics research, vol. 22, no. 3, pp. 156–163, 2016.

[2] M. H. Mohammed, M. N. Kadhim, D. Al-Shammary, and A. Ibaida, “Novel Voice Signal Segmentation Based on Clark Distance to Improve Intelligent Parkinson Disease Detection,” Journal of Voice, 2025.

[3] P. Manickam et al., “Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare,” Biosensors, vol. 12, no. 8, p. 562, 2022.

[4] A. A. Laklook, S. Khosroabadi, and A. H. Al-fatlawi, “A Special Design of Job Dropout Faces Detection and Recognition System (JDFDRs),” presented at the 2021 International Conference on Advanced Computer Applications (ACA), IEEE, 2021, pp. 138–143.

[5] M. N. Kadhim, A. H. Mutlag, D. A. Hammood, and N. B. H. Ismail, “Identification of Vehicle Logos in Deep Learning: A Comprehensive Survey,” Journal of Techniques, vol. 7, no. 1, pp. 37–47, 2025.

[6] S. S. Baawi, M. N. Kadhim, and D. Al-Shammary, “Efficient feature selection based on Gower distance for breast cancer diagnosis,” Journal of Electronic Science and Technology, vol. 23, no. 2, p. 100315, 2025.

[7] S. M. Abdulkhudhur, S. M. Abboud, A. H. Najim, M. N. Kadhim, and A. A. Ahmed, “A Hybrid Deep Belief Cascade-Neuro Fuzzy Approach for Real-Time Health Anomaly Detection in 5G-Enabled IoT Medical Networks.,” International Journal of Intelligent Engineering & Systems, vol. 18, no. 5, 2025.

[8] A. R. Hamad, S. M. Baraa Alsabti, A. H. Najim, and M. N. Kadhim, “A Hybrid Feature Selection and Machine Learning Approach for Parkinson’s Disease Detection from Voice Signals in IoT-Enabled 6G Networks.,” International Journal of Intelligent Engineering & Systems, vol. 18, no. 5, 2025.

[9] Z. H. Hashim Albohayah, S. B. Abed, A. J. Mahdi, M. N. Kadhim, and A. H. Najim, “Ch-PSO: A Novel Embedded Method based on PSO and Chebyshev Distance for Enhanced Epileptic Seizure Classification Using EEG Brain Signals.,” International Journal of Intelligent Engineering & Systems, vol. 18, no. 5, 2025.

[10] S. L. Alzamili, S. S. Baawi, M. N. Kadhim, D. Al-Shammary, and A. Ibaida, “Efficient feature selection based on Ruzicka similarity for EEG diagnosis,” International Journal of Information Technology, pp. 1–15, 2025.

[11] C. Avula and S. Bachala, “A Deep Feature Ensemble Framework for Intrusion Detection in Internet of Medical Things,” Engineering, Technology & Applied Science Research, vol. 15, no. 5, pp. 26783–26791, 2025.

[12] A. Salehpour, M. Norouzi, M. A. Balafar, and K. SamadZamini, “A cloud-based hybrid intrusion detection framework using XGBoost and ADASYN-Augmented random forest for IoMT,” IET Communications, vol. 18, no. 19, pp. 1371–1390, 2024.

[13] S. Farhan, J. Mubashir, Y. U. Haq, T. Mahmood, and A. Rehman, “Enhancing network security: an intrusion detection system using residual network-based convolutional neural network,” Cluster Computing, vol. 28, no. 4, p. 251, 2025.

[14] H. Goumidi and S. Pierre, “Real-Time Anomaly Detection in IoMT Networks Using Stacking model and a Healthcare-Specific Dataset,” IEEE Access, 2025.

[15] A. Khan, M. Rizwan, O. Bagdasar, A. Alabdulatif, S. Alamro, and A. Alnajim, “Deep Learning-Driven Anomaly Detection for IoMT-Based Smart Healthcare Systems.,” CMES-Computer Modeling in Engineering & Sciences, vol. 141, no. 3, 2024.

[16] M. A. Umar, Z. Chen, K. Shuaib, and Y. Liu, “Effects of feature selection and normalization on network intrusion detection,” Data Science and Management, vol. 8, no. 1, pp. 23–39, 2025.

[17] Z. Xia, S. He, C. Liu, Y. Liu, X. Yang, and H. Bu, “PSO-GA Hyperparameter Optimized ResNet-BiGRU Based Intrusion Detection Method,” IEEE Access, 2024.

[18] S. Moualla, K. Khorzom, and A. Jafar, “Improving the Performance of Machine Learning-Based Network Intrusion Detection Systems on the UNSW-NB15 Dataset,” Computational Intelligence and Neuroscience, vol. 2021, no. 1, p. 5557577, 2021.

[19] M. N. Kadhim, A. H. Mutlag, and D. A. Hammood, “Multi-models Based on Yolov8 for Identification of Vehicle Type and License Plate Recognition,” presented at the National Conference on New Trends in Information and Communications Technology Applications, Springer, 2023, pp. 118–135.

[20] S. S. Mahmood, M. A. Hasan, A. Al-bosham, A. H. Al-Fatlawi, M. S. Abd Al-Ameer, and H. Najm, “Efficient Emotional State Classification based on Bayesian Quantile Regression and PSO Using EEG Brain Signal.,” International Journal of Intelligent Engineering & Systems, vol. 18, no. 6, 2025.

[21] A. T. Albu-Salih, M. Y. Jumaah, A. H. Al-Fatlawi, and H. Najm, “Efficient Hybrid Feature Engineering and Supervised Learning Approach for Network Traffic Classification in Intrusion Detection Systems.,” International Journal of Intelligent Engineering & Systems, vol. 18, no. 6, 2025.

[22] M. H. Mohammed, M. N. Kadhim, D. Al-Shammary, and A. Ibaida, "EEG-Based Emotion Detection Using Roberts Similarity and PSO Feature Selection," IEEE Access, 2025.

[23] A. L. Albukhnefis, A. A. Sakran, A. S. Mahe, M. I. Mousa, and A. M. Mahdi, "Hybrid Intrusion Detection Systems Based Mean-Variance Mapping Optimization Algorithm and Random Search.," International Journal of Intelligent Engineering & Systems, vol. 16, no. 5, 2023.

[24] M. Sadiq, M. N. Kadhim, D. Al-Shammary, and M. Milanova, "Novel EEG feature selection based on hellinger distance for epileptic seizure detection," Smart Health, vol. 35, p. 100536, 2025.

[25] R. Malik, R. M. Alsharfa, B. K. Mohammed, A. H. Al-Fatlawi, M. S. Abd Al-Ameer, and H. Najm, "A Novel Taneja Distance-based Classifier with PSO-Optimized Feature Selection for Efficient 5G Network Slicing.," International Journal of Intelligent Engineering & Systems, vol. 18, no. 6, 2025.

[26] M. N. Kadhim, D. Al-Shammary, and F. Sufi, "A novel voice classification based on Gower distance for Parkinson disease detection," International Journal of Medical Informatics, vol. 191, p. 105583, 2024.

[27] H. H. Al-Kazzaz, M. J. Hazar, A. Naser, S. A. Razzaq, A. H. Al-Fatlawi, and S. A. Fadhil, "A Hybrid TD-PSO Feature Selection Approach for Accurate Arrhythmia Classification based on ECG Heart Signals.," International Journal of Intelligent Engineering & Systems, vol. 18, no. 7, 2025.

[28] M. N. Kadhim, D. Al-Shammary, A. M. Mahdi, and A. Ibaida, "Feature selection based on Mahalanobis distance for early Parkinson disease classification," Computer Methods and Programs in Biomedicine Update, vol. 7, p. 100177, 2025.

[29] M. Sadiq, M. N. Kadhim, D. Al-Shammary, and M. Milanova, "Novel EEG classification based on hellinger distance for seizure epilepsy detection," IEEE Access, 2024.

[30] W. H. M. Kurdi, H. A. Rassool, and A. H. Al-fatlawi, "Evaluation patterns and algorithm for cancer identifications using dynamic clustering," Periodicals of Engineering and Natural Sciences (PEN), vol. 9, no. 2, pp. 462–470, 2021.

[31] M. N. Kadhim, A. H. Mutlag, and D. A. Hammood, "Vehicle detection and classification from images/videos using deep learning architectures: A survey," presented at the AIP Conference Proceedings, AIP Publishing LLC, 2024, p. 020034.

[32] D. Al-Shammary, M. N. Kadhim, A. M. Mahdi, A. Ibaida, and K. Ahmed, "Efficient ECG classification based on Chi-square distance for arrhythmia detection," Journal of Electronic Science and Technology, vol. 22, no. 2, p. 100249, 2024.

[33] S. L. Kailan, W. H. Madhloom Kurdi, A. H. Najim, and M. N. Kadhim, "Efficient ECG Classification Based on Machine Learning and Feature Selection Algorithm for IoT-5G Enabled Health Monitoring Systems.," International Journal of Intelligent Engineering & Systems, vol. 18, no. 1, 2025.

[34] M. P. Raghunath et al., "PCA and PSO based optimized support vector machine for efficient intrusion detection in internet of things," Measurement: Sensors, vol. 37, p. 101806, 2025.

[35] W. H. Madhloom Kurdi, I. A. Alzuabidi, A. H. Najim, M. N. Kadhim, and A. A. Ahmed, "Efficient Two-Stage Intrusion Detection System Based on Hybrid Feature Selection Techniques and Machine Learning Classifiers.," International Journal of Intelligent Engineering & Systems, vol. 18, no. 3, 2025.

[36] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," Scientific Reports, vol. 15, no. 1, p. 1554, 2025.