Minimax Theory and its Applications

Volume 11 (2026), No. 5s, 89-104

An Adaptive Minimax Risk Optimization Framework for Robust Deep Learning-Based Cyberattack Detection in Heterogeneous IoT Architectures

Raj Anand Sundaramoorthy[1*], Kalpana Devi Perumal[2], Katukojwala Praveen Kumar[3], Ajith KrishnaRaghuraman[4], KoteeswaranSeerangan[5], Nalini Manogaran[6]

[1]School of Computing, Sastra Deemed University,Thanjavur-613401, Tamil Nadu, India.
[2]Department of ECE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi,Chennai – 600 062, Tamil Nadu, India.
[3] Department of Information Technology, Kakatiya Institute of Technology and Science,Warangal-506009,Telangana, India.
[4]Data Engineer, Amazon, Boston, Massachusetts, United States.
[5]Department of Computer Science and Engineering, R. M. K. Engineering College (Autonomous),Kavaraipettai - 601206, Tamil Nadu, India.
[6]Department of CSE (Cyber Security), S.A. Engineering College (Autonomous), Chennai – 600077, Tamil Nadu, India.
Email: rajanand@cse.sastra.ac.in, drkalpanadevip@veltech.edu.in, kpk.it@kitsw.ac.in, ajithkrishna1807@gmail.com,skn.cse@rmkec.ac.in,drnalini@saec.ac.in

Abstract
The increasing deployment of heterogeneous Internet of Things has expanded the cyberattack surface, creating significant challenges for reliable network security and malicious traffic detection. Conventional deep learning-based intrusion detection approaches primarily optimize average classification performance, which may limit their robustness against variations and disturbances in network traffic features. This study proposes an Adaptive Minimax Risk Optimization Framework for robust deep learning-based cyberattack detection in heterogeneous IoT architectures, designated as MAMIR-Net. The proposed methodology utilizes the CIC IoT-DIAD 2024 dataset and incorporates data preprocessing, missing and infinite value handling, feature normalization, and dataset partitioning. The framework integrates adaptive feature learning to identify informative network traffic characteristics, Minimax-based robust optimization to minimize classification loss under bounded input perturbations, and an intrusion classification module to distinguish benign and malicious traffic. Its effectiveness is investigated through binary and multiclass classification, convergence analysis, robustness evaluation, computational assessment, and component-wise ablation experiments. The reported results demonstrate that the complete MAMIR-Net configuration achieves 97.91% accuracy, 97.68% precision, 97.12% recall, and 97.90% F1-score. Furthermore, the worst-case classification loss decreases from 0.184 in the baseline configuration to 0.108 in the complete framework, representing an approximately 41.3% reduction. Comparative evaluation further reports 97.91% accuracy and a 97.90% F1-score against selected existing approaches. These findings highlight the potential of combining adaptive feature learning and Minimax risk optimization to enhance classification performance and robustness against bounded feature disturbances. The proposed framework provides a promising direction for developing reliable and adaptive cyberattack detection systems in heterogeneous IoT environments.

Keywords: Minimax Risk Optimization; Cyberattack Detection; Deep Learning; Adaptive Feature Learning; Robust Optimization; Heterogeneous IoT Architectures; Network Security.

I. Introduction

A. Background and Motivation

Internet of Things (IoT) Networks are increasingly becoming heterogeneous due to the growing number of smart devices, industrial systems, and distributed communication infrastructures connected to the Internet(Ahmed et al., 2023; Alabadi et al., 2022).They constantly share massive amounts of data with each other using various communication protocols, leading to intricate traffic flow and some increasing risk of cybersecurity issues(Tariq et al., 2023).Therefore, DDOS, Spoofing, Reconnaissance and BF attacks are great

threats to IoT network reliability and integrity(Pakmehr et al., 2024; Sefati et al., 2025).The use of ML and DL algorithms has seen significant interest in the field for detecting malicious traffic by extracting and training features automatically(Genuario et al., 2024; Wang & Thing, 2023).However, if the network parameters change there are unexpected disturbances in the input features, there is a risk of degradation of the conventional learning approaches(Umar & Jordanov, 2026).Moreover, unbalanced attacks distributions may impact on less-represented attack category identification.Thus, combining Minimax optimization and adaptive feature learning is a potential approach for enhancing the worst-case classification accuracy, robustness and computational efficiency in heterogeneous IoT intrusion detection systems(Wang et al., 2024).

B. Existing Problem

Although ML-based IoT intrusion detection has made significant advances, several issues still need to be addressed to enable the reliable classification of cyberattacks in such uncertain network environment(Alfahaid et al., 2025; Kikissagbe & Adda, 2024).Typically, conventional deep learning models minimize average training loss, it is not suitable to capture worst-case classification errors when the traffic characteristics of networks vary(Hameed et al., 2022).Furthermore, sensitivity to bounded feature disturbances may lead to a decrease in prediction accuracy, especially if malicious traffic follows a pattern that differs from the patterns learnt during training(Li et al., 2025).In addition, the imbalance of the distribution of attack categories makes multiclass classification more difficult as it reduces the learning capability for the minority attack categories(Jyoti et al., 2026).Existing studies explore adversarial learning, adaptive feature selection and Minimax-based optimization incorporation into a single, efficient deep learning system is limited (Maharajan et al., 2026). Such constraints drive the development of an adaptive Minimax risk optimization framework that enhances classification reliability explicitly accounting for worst case feature disturbances and heterogeneous IoT traffic characteristics.

C. Research Objectives

1. To develop a Minimax-based robust learning architecture that minimizes worst-case classification loss under bounded IoT traffic disturbances.
2. To introduce an adaptive feature representation mechanism for effectively learning discriminative characteristics from heterogeneous IoT network traffic.
3. To evaluate cyberattack detection performance by examining classification accuracy, robustness against feature disturbances, and efficiency.

D. Main Contributions

1. Minimax-Based Risk Optimization: A Minimax optimization strategy is formulated to minimize worst-case classification loss under bounded input disturbances, improving the robustness of IoT cyberattack detection.
2. Adaptive Feature Representation: An adaptive feature learning mechanism is developed to capture discriminative traffic characteristics and improve the representation of heterogeneous IoT network observations.
3. Robust Deep Learning Architecture: An integrated learning framework is designed by combining adaptive feature extraction with Minimax-based optimization for reliable cyberattack classification.
4. Binary and Multiclass Detection: The proposed framework is evaluated for benign-versus-malicious traffic identification and multiclass attack classification using the CIC IoT-DIAD 2024 dataset.
5. Comprehensive Performance Evaluation: Experiments are conducted to investigate the effectiveness and individual contributions of the proposed framework

II. Related Work

A.ML-Based IoT Intrusion Detection

To tackle the issue of class imbalance in multiple network traffic, Park et al. (2023)suggested a generative AI-based network intrusion detection system. The experiments on IoT-23 dataset showed better performance in multiclass intrusion detection, with the G-DNNAE model having an accuracy of 93.2%, a precision of 70.2%, and an F1 Score of 80% in the DDoS class. Yang et al. (2025)proposed a DDoS detection framework using reinforcement learning in the consumer IoT healthcare system. They used off-policy PPO, class-aware reward augmentation, GAN for data generation and BOHB for hyperparameter optimization. The proposed framework was evaluated using KDDCup99, ISCX UNB, CICDDoS, and DARPA datasets, achieving accuracy and F-measure values of 90.498% and 89.286%, 93.186% and 91.896%, 92.403% and 90.285%, and 92.849% and 92.790%, respectively.

To detect DDoS attacks by learning the discriminative traffic characteristics and spatial-temporal dependencies, Irankunda et al. (2026)have proposed a hybrid DDoS detection framework using XGBoost-based feature selection followed by CNN-LSTM architectures. The accuracy achieved during the cross domain evaluation was 93.33% on CICIoT2023. The results of these studies show that these generative learning, reinforcement learning and hybrid DL architectures are effective in enhancing IDS for IoT applications. Their main optimization techniques, however, do not explicitly minimize worst-case classification risk under a variety of heterogeneous network conditions, but rather feature selection, class imbalance, or predictive performance.

B. Deep Learning-Based Anomaly Detection in IoT and IIoT Networks

Chen et al. (2024)introduced an optimized DL framework for anomaly detection in IIoT, called MIX_LSTM. To mitigate the computational burden they chose to use feature selection using XGBoost with multiple importance thresholds to remove less informative features. An optimized loss function was also added to overcome the

problem of class imbalance, highly similar attack categories, and training stability. For UNSW-NB15, experiments with UNSW-NB15 and NSL-KDD yielded a false alarm rate of 0.084, AUC-ROC of 0.984 and AUC-PR of 0.988.STGaAN were introduced for anomaly detection in industrial IoT sensor networks by Fan et al. (2024). The proposed architecture used sensor dependency graphs to build dependency relationships between sensors and combined the gated graph attention network and temporal convolutional network to capture spatial and temporal relationships. Aiming to improve anomaly detection, joint reconstruction and prediction losses were adopted. STGaAN achieved 98.82% precision, 73.13% recall and an F1 score of 84.06% on the SWaT dataset.

Han et al. (2026)presented a hybrid quantum-classical anomaly detection algorithm that combines QRBF kernel with ANNLoG classifier. Hyperparameter tuning was performed using the BOTOX and Min-Max normalization was applied to UNSW-NB15, CIC-IDS2017 and ToN-IoT datasets. The classification accuracy for the ANNLoG model was 99.9%, 99.8% and 99.7% respectively. On CIC-IDS2017, it also reported MSE, MAE, and RMSE values of 0.0010, 0.0080, and 0.0316, respectively. These investigations together suggest that the optimization of features, the representation in space and time, and hybrid learning architectures are crucial to the problem of anomaly detection in IoT. However, it is still an important research direction to develop adaptive learning models that explicitly consider worst case uncertainty and adversarial variations. Nguyen and Park (2026)pointed out that GNNs have high closed set accuracy, but fail to detect zero-day attacks. Similarly, Euclidean distance doesn't take class-conditional covariance into account, as does OpenMax. To set rejection boundaries without a hand-tuned cutoff, they have proposed MaGOS-IDS, the application of an edge-aware GCN, a regularized Mahalanobis distance per class and finally the application of per-class EVT tail calibration. On CIC-IDS-2017, MaGOS-IDS achieved 95.86% accuracy and 95.64% macro-F1; and on UNSW-NB15, superior to the baseline of Euclidean OpenMax at 0.848. The authors recognize the constraints of snapshot-level labelling, the estimation of covariances for rare classes, the evaluation of the system in the offline setting, and the lack of testing of the system for robustness against adversarial evasion and concept drift.

C. Minimax-Based and Robust Optimization Approaches

Gazzan and Sheldon (2023)introduced a loss function called BGM in combination with GAN for early detection of ransomware, specifically in pre-encryption phase of ransomware attacks, focusing on polymorphic and metamorphic patterns. The method they used gradually reduced the maximum loss between the generator and discriminator to make it possible to produce artificial attack patterns similar to the pre-encryption data distributions. Patterns were generated and added to the original training data set in order to boost detection capabilities for changing ransomware behavior. Experimental results showed maximum accuracy of 0.98, maximum recall of 0.96 and maximum FPR of 0.14. In an extension of the Context-Aware Sensor-Cloud Architecture with Integrated Machine Learning Analytics and Dynamic Model Orchestration (CASC-MO), Jayalakshmi et al. (2026)proposed a minimax approach. The framework incorporated context-specific Isolation Forest models, categorical context descriptors, contamination calibration and a global fallback model. The candidate detector was chosen using its minimax selection mechanism which chose the detector with the lowest maximum validation loss over various operational contexts. For experiments on a simulated smart-building dataset with 4320 observations across 5 sensor channels, an AUC-ROC of 0.8824 and recall of 82.81% was obtained. Nevertheless, the framework was not able to detect drift anomalies and the assessment was limited to simulated data and one experimental run.

Maharajan et al. (2026)proposed an adaptive noise-aware hybrid quantum intrusion detection framework (ANHQ-IDS) which combines the resource-constrained feature selection, quantum feature encoding and a variational quantum classifier. In the framework, the feature relevance, redundancy, stability and quantum encoding costs were jointly taken into consideration under a fixed number of qubits. Under exact simulation on CIC-IDS2017, ZZ-encoded variational quantum classifier performed logistic regression scored 0.502 macro-F1 and Random Forest scored 0.964 macro-F1. The framework also explored degraded performance in the presence of depolarizing noise and readout noise. The aforementioned studies demonstrate the importance of Minimax optimization and robust learning in the fields of ransomware detection, context-aware anomaly detection and network security. The existing methods all, however, do not have a single framework to cover adaptive deep feature learning, heterogeneous IoT traffic, and systematic worst case risk optimization.

D. Research Gap and Motivation for Proposed Framework

The IoT intrusion detection systemshave some limitations in intrusion classification in uncertain and changing network environments. Most of the conventional DL models focus mainly on optimizing average classification accuracy while neglecting to consider the worst case prediction errors **(Irankunda et al., 2026; Park et al., 2023)**. While graph-based and spatio-temporal methods enhance traffic representation, the robust performance against adversarial disturbances and distribution variations have not been thoroughly studied **(Nguyen & Park, 2026)**. The existing Minimax-based methods focus more on the problem of GAN optimization and context-dependent anomaly detection instead of a single framework covering adaptive DL for heterogeneous IoT traffic. In addition, it is difficult to address problems of computational complexity and imbalanced attack types. To address issues, this study proposes a novel Adaptive Minimax Risk Optimization Framework that combines Adaptive Feature Learning and Worst-case Loss Minimization for robust multiclass cyberattack detection.

III. Materials and Methods

The proposed model materials, characteristics of the dataset, preprocessing, and experimental configurations used to create the proposed Minimax-optimized adaptive machine learning framework for IoTID are presented. The CIC IoT-DIAD 2024 dataset is chosen for the study of benign and malicious traffic on the network in heterogeneous IoT environments. Data collection and pre-processing are first implemented to ensure that the data is consistent and can be used numerically. Then, class distribution analysis and partitioning of the dataset lay the groundwork for model development and evaluation in the experiments. The computed processed dataset is the structured representation of the network traffic, for adaptive feature learning, Minimmax based robust optimization, and intrusion classification.

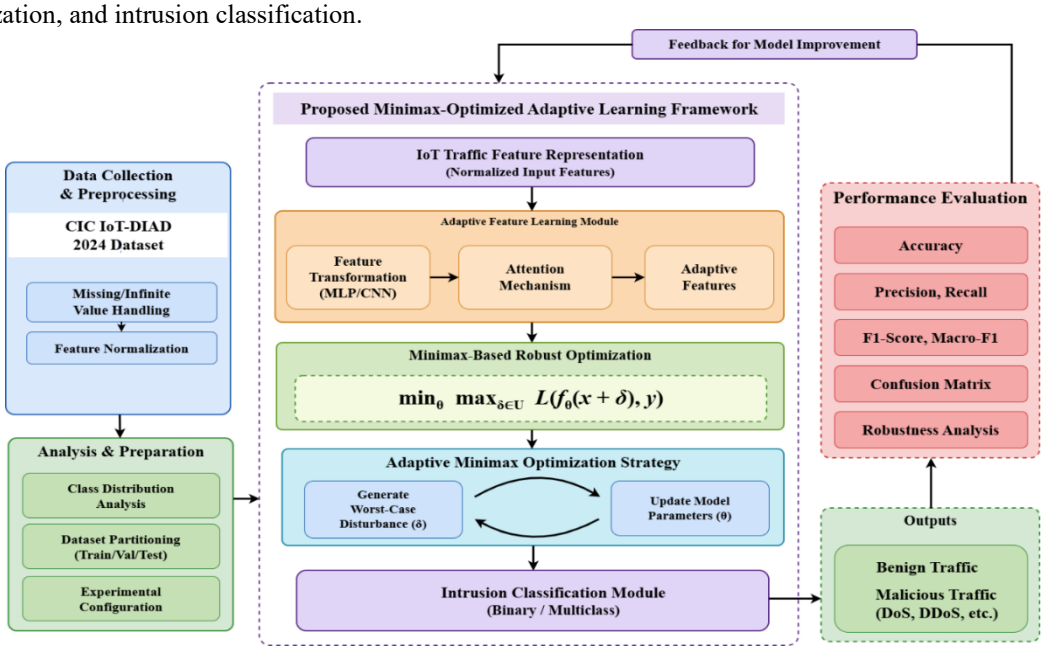

Figure 1. Workflow of the Proposed Minimax-Driven Learning Methodology for IoT Security

The framework shown in Figure 1, which includes data gathering, data pre-processing, data class distribution analysis, and data splitting. Adaptive feature learning and Minimax-based robust optimization improve the intrusion detection, while the classifier distinguishes between benign and malicious traffic.

3.1 Data Collection

The CIC developed the CIC IoT-DIAD 2024 dataset, which is chosen for this research to assess the proposed machine learning framework optimized for Minimax. This data is network traffic from a variety of diverse Internet of Things (IoT) devices operating in benign and malicious environments(n.d.). It covers various attack scenarios such as DoS, Distributed DoS, Reconnaissance, Spoofing, Brute Force and Web Based Attacks. The data set contains network traffic characteristics that can be used for machine learning-based intrusion detection using flow and packet information. It is possible to do binary and multiclass classification experiments using the collected records, which are used to detect abnormal network behaviour and decide the difference between legitimate traffic and malicious traffic.

3.2 Data Preprocessing

Data Pre-processing is a vital step in the proposed Minimax-optimized ML framework for IoT ID system. The CIC IoT-DIAD 2024 dataset includes a mix of network traffic data that can include missing network data, infinite numerical data, and differing measurement scales. This can have an impact on model training, classification performance and Minimax optimization. Hence, these are handling of missing values and features normalization to enhance the data quality, numerical stability and uniformity of data inputs into the proposed intrusion detection model.

3.2.1 Missing-Value and Infinite-Value Handling

Handling missing values and infinite values are done to guarantee the reliability of the CIC IoT-DIAD 2024 network traffic features. Several problems can cause missing entries in the record of flows: incomplete flow records, or infinite values during the computation of statistical traffic features (e.g., flow rates and ratios). The missing and infinite values are firstly identified and replaced with median of the respective feature. The replacement method maintains the data's number line structure but minimizes the effect of outlying values. This preprocess prevents from the numerical instability in the adaptive feature learning and Minimax based optimization. The replacement operation is represented as in equation (1).

$$x_{ij}^{*} = \begin{cases} \text{Median}(X_j), & x_{ij} \text{ is missing or infinite} \\ x_{ij}, & \text{otherwise} \end{cases} \quad (1)$$

Where x_{ij}^{*}: Corrected value of the j-th feature in the i-th record, x_{ij}: Original feature value, X_j: All valid observations of the j-th feature, $\text{Median}(X_j)$: Median of the valid observations of that feature.

3.2.2 Feature Normalization

The numerical features of the network traffic are normalized to a common range using feature normalization method before training the proposed machine learning-based model using the Minimax optimization. The CIC IoT-DIAD 2024 data set has some features that have large numbers and some that have small numbers, and this could lead to some attributes being more influential in the learning process. So, Min-Max normalisation is used to normalise each numerical feature between 0 and 1. This transformation also has the advantage of making the input features more uniform and helps to ensure the stability of the gradient-based optimization process during the training of the model. Normalization parameters are then applied to the validation and testing data sets, using the same parameters used in the training set. Min-Max normalization can be defined as in equation (2).

$$x_{ij}^{norm} = \frac{x_{ij} - x_j^{min}}{x_j^{max} - x_j^{min}} \qquad (2)$$

Where x_{ij}^{norm}: Normalized value of the j-th feature in the i-th record, x_{ij}: Original feature value, x_j^{min}: Minimum training value of the j-th feature, x_j^{max}: Maximum training value of the j-th feature.

3.3 Class Distribution Analysis

The benign and malicious network traffic in CIC IoT-DIAD 2024. The dataset might have multiple categories of attacks over IoT devices as potentially different numbers of traffic observations. Hence, distribution of individual classes is crucial to discover the class imbalance and gain insight into the contribution of each class towards intrusion detection. Where x_i is the vector of features for network traffic of the ith sample, and y_i is the class label of the ith sample. The number of observations in class c as in equation (3).

$$N_c = \sum_{i=1}^{N} \mathbb{I}(y_i = c) \qquad (3)$$

Here, N_c denotes the total observations of class c, N represents the total dataset size, and $\mathbb{I}(\cdot)$ is an indicator function that returns one when the condition is true and zero otherwise. The proportional representation of each class is determined as in equation (4).

$$P_c = \frac{N_c}{N} \times 100 \qquad (4)$$

where P_c indicates the percentage distribution of class c. To evaluate the degree of class imbalance, the imbalance ratio is calculated as in equation (5).

$$IR = \frac{\max_{c \in C} N_c}{\min_{c \in C} N_c} \qquad (5)$$

where IR represents the imbalance ratio and C denotes the complete set of class labels. A larger value indicates a greater difference between the majority and minority classes.

The class distribution is analyzed using frequency analysis and graphically to detect the underrepresented attack categories. A binary configuration is considered as well as a multiclass configuration. In binary classification all malicious traffic is classified as a single class and it is separated from benign traffic, while multiclass classification retains the individual attack labels. This analysis is especially relevant of the proposed minimax framework as minority attack classes can be involved in disproportionate misclassification errors in the worst case. Hencethe overall classification accuracy to ensure that the proposed model is not biased towards the dominant traffic categories.

3.4 Dataset Partitioning

The purpose of partitioning is to create several independent partitions for training the model, validating the parameters and evaluating the model performance. The dataset is split into training, validation and testing sets to evaluate the capability of the proposed Minimax-optimized adaptive learning framework to generalize. For this study, a partitioning strategy of 70:15:15 is adopted in which 70% of the observations are used for training, 15% for validation, and 15% for testing. The training subset is employed for training the model parameters and to optimize the Minimax objective, and the validation subset is used for hyperparameter selection and monitoring convergence. The testing subset is only used to test the final trained model. The partitioning of the data is shown as in equation (6).

$$D = D_{train} \cup D_{val} \cup D_{test} \quad (6)$$

where D_{train}, D_{val}, and D_{test} represent the training, validation, and testing subsets, respectively. The three subsets must satisfy the following mutually exclusive condition as in equation (7).

$$D_{train} \cap D_{val} \cap D_{test} = \emptyset \quad (7)$$

The number of observations assigned to each subset is determined as in equation (8).

$$N_s = \alpha_s N, \qquad \sum_{s \in \{train,val,test\}} \alpha_s = 1 \qquad (8)$$

where N_s denotes the number of observations in subset s, α_s represents its allocation proportion, and N indicates the total number of observations.

3.5 Experimental Data Configuration

Images and labels from experimental data are configured to represent the type of input and the target labels and classification parameters used to test the proposed Minimax-optimized adaptive learning framework.Images and labels from the experimental data are configured for input representation, target labels and classification parameters for evaluation of the proposed Minimax-optimized adaptive learning framework. The CIC IoT-DIAD 2024 dataset is setup for two different complementary classification problems: Binary Intrusion Detection and Multi-class Attack Recognition. The binary configuration can differentiate between legitimate IoT traffic and malicious network activities and gives a general estimation of the intrusion detection capability.Let the matrix of the input features be given as in equation (9).

$$X \in \mathbb{R}^{N \times d} \quad (9)$$

where X denotes the normalized network traffic feature matrix, N represents the number of observations, and d indicates the number of selected numerical input features. For binary classification, the target label is defined as in equation (10).

$$y_i^{(b)} = \begin{cases} 0, & \text{Benign traffic} \\ 1, & \text{Malicious traffic} \end{cases} \quad (10)$$

Here, $y_i^{(b)}$ represents the binary target label of the i-th network traffic observation. For multiclass classification, the original attack-category labels are retained and encoded into integer class identifiers.

IV. Proposed Minimax-Optimized Adaptive Learning Framework

The proposed Minimax-Optimized Adaptive Learning Framework is designed detection in IoT networks with multiple heterogeneous network types by leveraging the CIC IoT-DIAD 2024 dataset. Combines adaptive feature learning, worst case disturbance optimization, and multiclass classification, in order to detect benign and malicious network traffic. The proposed method is based on Minimax optimization, which in addition to optimizing average training loss, takes into account the errors in the classification process under admissible feature disturbances, unlike the traditional machine learning methods. The architecture comprises of traffic feature representation, adaptive feature extraction, Minimax based robust optimization and intrusion classification module. The mathematical formulation and computational operations of each of them are explained in the following subsections.

4.1 Overall Framework Architecture

The overall architecture of proposed framework is the four-stage architecture of processing to obtain robust intrusion detection in IoT. The feature representation stage receives the network traffic observations from the CIC IoT-DIAD 2024 in a normalized form at first. The adaptive feature learning module has trainable transformations and attention-based feature weighting to extract informative features from the input traffic. Next, the optimization module (Minimax) determines locations of difficult feature disturbances and adjusts the model parameters so as to minimize the corresponding worst case classification error. Finally, the intrusion classification module is able to produce the prediction of benign / malicious traffic and individual attack categories. The overall architecture sets up an integrated learning process where adaptive feature extraction and powerful optimization optimize the classification reliability. Its mathematical representation is given as in equation (11).

$$\hat{Y} = F_{\Theta}(X; \delta) \quad (11)$$

where X denotes the normalized IoT traffic input, $\hat{Y}$ represents the predicted output, Θ indicates the complete set of trainable parameters, δ denotes an admissible feature disturbance, and F_{θ} represents the complete proposed learning framework.

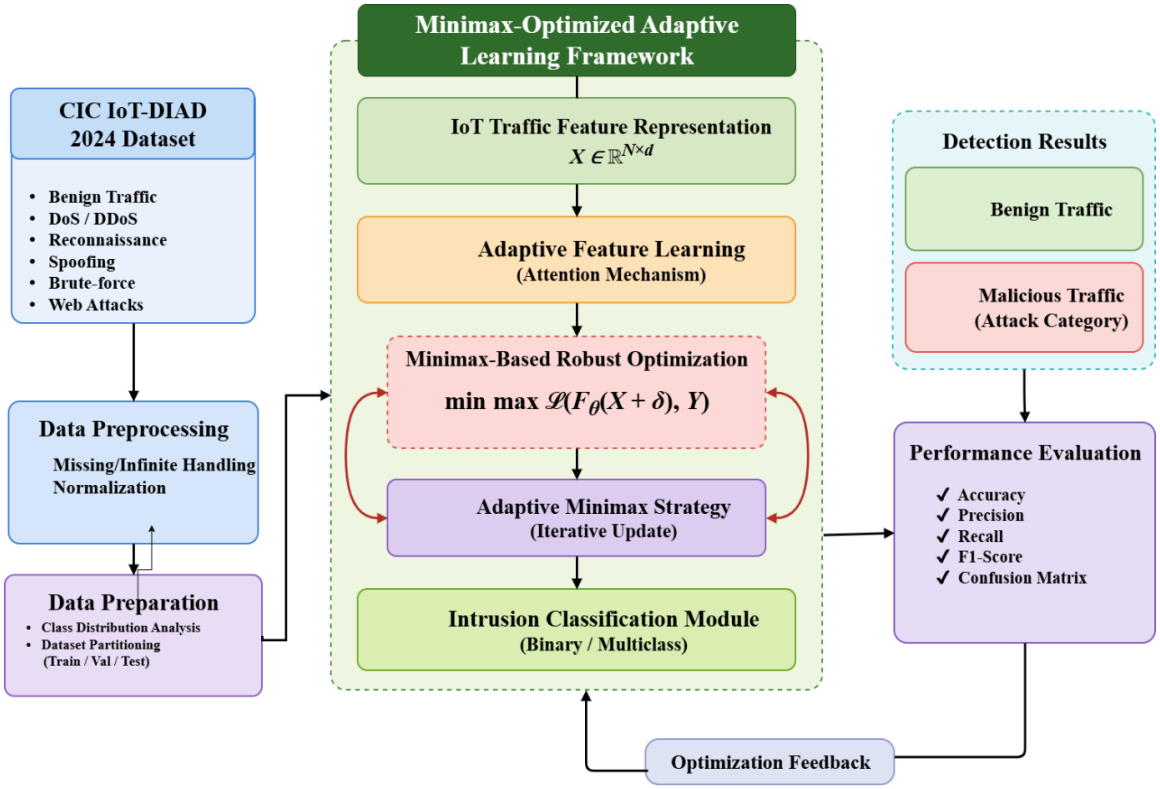

Figure 2. Internal Architecture of the Adaptive Feature Learning and Robust Minimax Optimization Mechanism

The proposed framework is illustrated in Figure 2, incorporating IoT traffic modeling, feature learning, and robust optimization using the Minimax approach. The iterative parameter tuning is utilized of the intrusions into either the benign or malicious categories.

4.2 IoT Traffic Feature Representation

The IoT traffic feature representation maps the preprocessed network observations to a structured numerical representation, which would benefit adaptive learning and Minimax optimization. Each observation comprises a number of numerical attributes that capture aspects of network communication such as available flow statistics, packet-related measurements and traffic information. Each traffic observation is represented as a feature vector, with the same representation throughout the experiments to ensure consistent input to the system. These are the feature vectors that are then fed into an adaptive feature learning module. In the representation, the relationship between the input attributes and the corresponding attack labels are maintained, making the representation suitable for binary and multiclass intrusion detection experiments. The individual traffic observation is represented as in equation (12).

$$x_i = [x_{i1}, x_{i2}, \ldots, x_{id}]^T \quad (12)$$

where x_i represents the i-th IoT traffic observation, x_{ij} denotes its j-th normalized feature, d indicates the total number of input features, and T denotes vector transposition.

4.3 Adaptive Feature Learning Module

The adaptive feature learning module is proposed to discover informative traffic features and create discriminative representation for intrusion classification. First, it projects the input feature vector with a trainable nonlinear projection. Attention-based weighting mechanism is then used to give different importance value to the extracted features. This mechanism allows for the proposed model to highlight informative traffic features and to mitigate the impact of less informative features. These attention weights are trained with back propagation, and are adjusted based on the classification goal. The adaptive representation that is generated is fed into the Minimax optimisation module, and the framework is thus able to learn traffic characteristics under various admissible disturbance situations. The feature transformation is nonlinear, and is represented as in equation (13).

$$h_i = \mathrm{ReLU}(W_h x_i + b_h) \quad (13)$$

where h_i represents the extracted feature representation, W_h denotes the trainable transformation matrix, b_h indicates the bias vector, and ReLU represents the nonlinear activation function. The adaptive attention weights are calculated as in equation (14).

$$a_{ij} = \frac{\exp(q_{ij})}{\sum_{k=1}^{d} \exp(q_{ik})} \quad (14)$$

where a_{ij} denotes the attention weight of the j-th feature, q_{ij} represents its learned attention score, and d indicates the number of input features. The final adaptive feature representation is obtained as in equation (15).

$z_i = a_i \odot h_i$ (15)

where z_i represents the adaptive feature vector, a_i denotes the attention-weight vector, h_i indicates the transformed feature vector, and $\odot$ represents element-wise multiplication. The dimensions of the attention and transformed feature vectors are aligned before multiplication.

4.4 Minimax-Based Robust Optimization

The core optimization element of the proposed framework is the robust optimization module that is based on the minimax approach. It focuses mainly to reduce the classification loss in presence of the worst case allowable disturbances to the IoT traffic features. In traditional learning approach, the learning performance is optimized based on the learning observation, while the proposed approach takes into account variations in the input feature space that may be difficult. The uncertainty set is defined to bound the perturbations within sensible feature ranges, and to ensure meaningful characteristics of network traffic. The inner maximization finds disturbances that make the classification loss larger, and the outer minimization modifies the trainable model parameters to minimize the maximum classification loss (worst-case error).The strong Minimax objective as in equation (16).

$\min_{\Theta} \max_{\delta \in \mathcal{U}} \frac{1}{N} \sum_{i=1}^{N} \mathcal{L}\left(F_{\Theta}(x_i + \delta), y_i\right)$ (16)

where Θ represents trainable model parameters, δ denotes the feature disturbance, $\mathcal{U}$ indicates the admissible uncertainty set, N represents the number of training observations, $\mathcal{L}$ denotes the classification loss, and y_i represents the actual class label. The inner maximization searches for challenging admissible disturbances, whereas the outer minimization determines parameters that reduce the worst-case classification loss.

4.5 Adaptive Minimax Optimization Strategy

Adaptive Minimax optimization strategy combines worst case disturbance generation and model parameter updating to realize robust learning. The parameters of the model are first set to initial values and the training data are given in mini-batches. The inner optimization process creates perturbed traffic samples that are difficult by maximizing the classification loss in the specified uncertainty set. The model parameters are then sequentially updated by gradient-based minimization of the estimated worst case loss, for the outer optimization. The two optimisation operations are then repeated for successive iterations until the convergence condition is met. The validation set is used to track learning progress and to choose an appropriate set of hyperparameters. The proposed framework utilizes this alternating optimization approach to enhance its classification performance, when subjected to bounded features disturbances. Alternating Parameter Update is represented as in equation (17).

$$\begin{aligned} \delta^{(t+1)} &= \Pi_{\mathcal{U}}\left(\delta^{(t)} + \eta_{\delta} \nabla_{\delta} \mathcal{L}\left(\Theta^{(t)}, \delta^{(t)}\right)\right), \\ \Theta^{(t+1)} &= \Theta^{(t)} - \eta_{\Theta} \nabla_{\Theta} \mathcal{L}\left(\Theta^{(t)}, \delta^{(t+1)}\right) \end{aligned} \quad (17)$$

where t represents the optimization iteration, η_{δ} denotes the disturbance ascent learning rate, η_{Θ} indicates the model learning rate, $\Pi_{\mathcal{U}}$ represents projection onto the admissible uncertainty set, and ∇ denotes the corresponding gradient. The disturbance update maximizes the loss, while the parameter update minimizes it.

4.6 Intrusion Classification Module

The intrusion classification module transforms the adaptive feature representation to final prediction of intrusion. The adaptive feature learning module produces a representation of these features which is passed to a fully connected classification layer that provides class scores for the traffic classes available. For multiclass classification a Softmax activation is used to get normalized class probabilities. For binary classification, the model is able to determine whether traffic is benign or malicious, while for multiclass classification, it can recognize individual attack types that may have been included in the data set. The estimated probability is the highest for the category that is predicted. The classification module hence carries out the last decision making process in the proposed framework and also the performance assessment of intrusion detection with independent testing observations.

4.7 Computational Complexity Analysis

The adaptation-induced complexity of the feature learning system, as well as the complexity induced by the Minimax based optimization. The number of training observations, input feature dimensions, model architecture, mini-batch size and inner optimization iterations are the main factors with respect to computational cost. The proposed Minimax model improves on conventional classification models by carrying out extra optimization steps to discover difficult feature disturbances. This means that the training process needs more computational power for multiple times of disturbance generation and model parameter updating. Let E be the number of epochs for training; K be the number of inner optimisation iterations; N_b be the size of the mini-batch; and C_f be the computational cost per evaluation of the model and per calculation of the gradients. The complexity of the training is approximately as in equation (18).

$$\mathcal{O}\left(EKN_bC_f\right) \quad (18)$$

The number of inner iterations of the optimization algorithm and complexity of adaptive learning architecture are factors that affect computational overhead. The inner Minimax loop isn't executed during inference, meaning the trained model can do feature transformation, attention weighting, and classification without ever needing to optimize the model. Thus, it is less costly to make inferences than to train. The amount of memory used is

determined by model parameters, intermediate feature representations, and mini-batches storage. These measurements will help to assess the feasibility of the proposed framework in resource-limited IoT networks.

V. Result and Discussion

The proposed MAMIR-Net framework for its classification performance, convergence behaviour, robustness and computational efficiency. The CIC IoT-DIAD 2024 dataset is used in experiments for both binary and multiclass IoT ID. The effects of adaptive feature learning and Minimax optimization are evaluated and demonstrated by conducting component-wise ablation experiments. Training curve and validation curve are analyzed to understand the convergence of the model, classification characteristics and confusion matrix analysis are employed to understand the effectiveness of detection per category of the attack. In addition, controlled feature disturbances are added to test the robustness of the framework with various levels of disturbances. Last, computational measurements were taken to evaluate the potential applicability of the framework to an IoT setting. The numerical results reported must agree with the experimental results.

A. Experimental Environment and Hyperparameter Configuration

The experimental environment is used to define the computational and algorithmic environments in which the proposed Minimax-Optimized Adaptive Machine Learning Framework are evaluated. To explore the model's intrusion detection ability in heterogeneous IoT network environments, the CIC IoT-DIAD 2024 dataset is used. The configuration for the implementation consists of the programming environment, deep learning framework, optimization algorithm, learning rate, batch size, and training duration. The Minimax optimization parameters which regulate the inner maximization and outer minimization processes are discussed in particular are shown in Table 1. These settings serve as a repeatable basis to investigate the convergence behaviour, classification performance and computational needs of the proposed framework.

Table 1. Experimental Setup

Parameter	**Experimental configuration**
Dataset	CIC IoT-DIAD 2024
Proposed framework	MAMIR-Net
Programming language	Python
Deep learning framework	PyTorch
Loss function	Cross-Entropy Loss
Batch size	128
Learning rate	0.001
Training epochs	100
Feature normalization	Numerical feature normalization
Minimax optimization	Gradient-based optimization
Inner optimization	Projected gradient ascent
Outer optimization	Gradient descent
Evaluation tasks	Binary and multiclass classification

B. Training Convergence and Optimization Stability

The convergence analysis shows how the proposed MAMIR-Net framework is learning during the training process. Training Loss and Validation Loss plots across the epochs, showing the typical decline in classification loss and the convergence of the training and validation processes. Minimax worst case loss convergence in iterations of the optimization are shown in Figure 3. The loss profile is decreasing to reflect the desired action of the outer minimization process: to minimize the disturbances that are admissible. These graphs are used together to analyze the optimization stability, learning consistency and efficiency of the proposed training strategy.

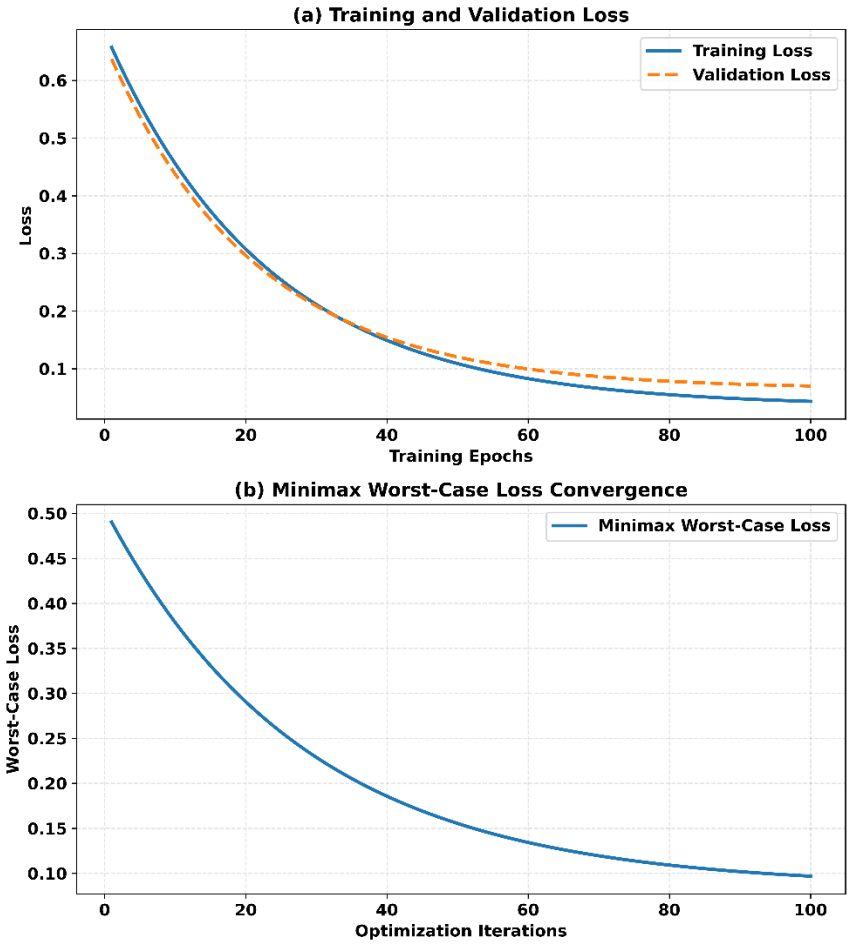

Figure 3. Training and Minimax convergence analysis

C. Data Preprocessing and Minimax Robustness Configuration

The preprocessing and robustness configurations set the data quality and uncertainty conditions for the evaluation of the proposed Minimax-based learning framework are shown in Table 2. Before feature normalization, infinite values and missing values are detected and dealt with to ensure consistency in numbers from the onset of learning. Parameters that normalize the numerical features are estimated from training data and applied to the validation and testing data. After pre-processing, perturbations within the bounds to normalized feature space to test the model's ability to withstand uncertainty in the input space. Various levels of disturbances are used to evaluate worst-case classification behaviour, keeping feature domain constraint at an appropriate level throughout the optimization process.

Table 2. Data preprocessing and Minimax-based robustness evaluation configuration

Component	Configuration
Missing-value identification	NaN detection
Missing-value treatment	Defined replacement or removal strategy
Infinite-value identification	Positive and negative infinity detection
Infinite-value treatment	Defined replacement or removal strategy
Feature normalization	Numerical feature normalization
Normalization parameter fitting	Training dataset
Validation transformation	Training-fitted normalization parameters
Testing transformation	Training-fitted normalization parameters
Outer optimization	Gradient descent
Robustness evaluation	Accuracy, Macro-F1, worst-case loss

D. Binary and Multiclass Classification Effectiveness

The classification performance analysis is performed for the proposed framework in binary and multiclass ID system are shown in Figure 4. The key metrics considered for identifying benign and malicious IoT traffic. The

results help recognize differences in the detection capability of individual classes of traffic and analyze its effect of heterogeneous traffic characteristics. The overall analysis quantifies the effectiveness of the proposed model in classifying attacks applied to IoT networks and their ability to detect various attacks.

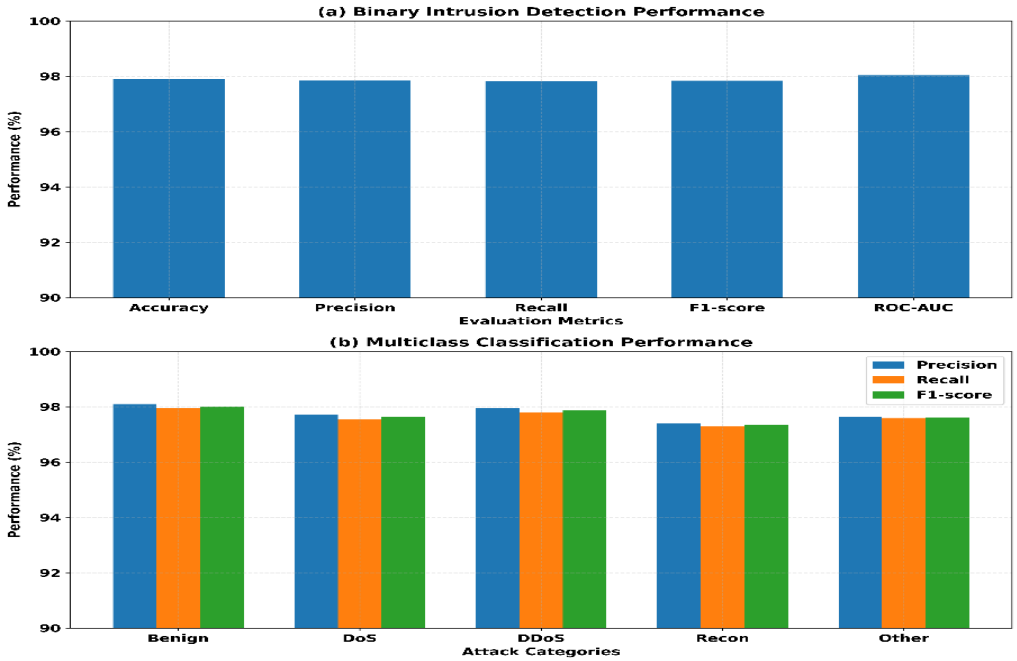

Figure 4. Binary and multiclass classification performance

E. Adaptive Feature Importance and Contribution Analysis

Adaptive feature importance reveals the contribution level of individual network traffic features in the suggested MAMIR-Net model frameworkare shown in Figure 5. The first subplot shows the contribution level of the primary traffic features like flow duration, packet size, number of flow bytes, and packet rate. The second subplot depicts the contribution level of secondary traffic features like number of TCP flags, inter-arrival time, and packet characteristics. Higher levels of feature importance reveal higher levels of contribution to the learned feature representation and classification. Such an approach helps detect discriminatory network traffic features regarding benign and malicious network traffic patterns. In addition, feature importance distribution reveals more about the adaptive learning approach.

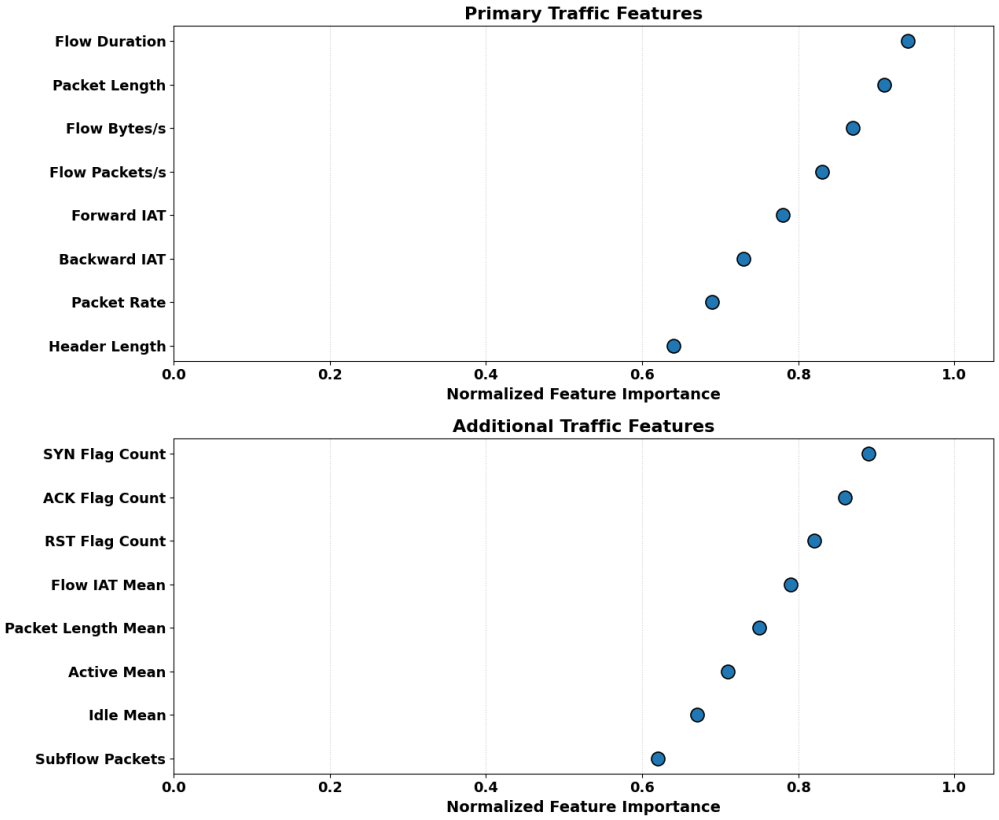

Figure 5. Feature Importance Ranking in MAMIR-Net

F. Multiclass Confusion Matrix Analysis

A multi class confusion matrix is also analyzed to further investigate the classification distribution of the proposed MAMIR-Net framework. Figure 6 shows correlation between actual and predicted IoT traffic categories, where it is possible to get a detailed view of the accuracy and inaccuracy of these classifications. Through this analysis it is possible to identify categories of attacks that have similar traffic characteristics and to assess the model's ability to differentiate between benign traffic and malicious traffic. The confusion matrix also gives some other indication of classification false-positive and false-negative behaviours.

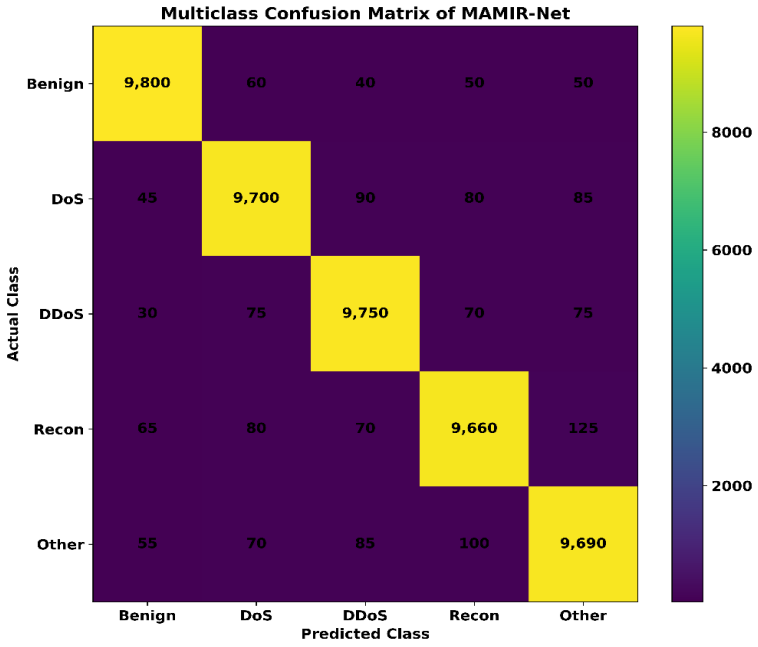

Figure 6. Confusion matrix of the proposed MAMIR-Net

G. Minimax-Based Robustness Evaluation

The robustness of the proposed framework is investigated to bounded feature-disturbance conditions to evaluate the effectiveness of Minimax optimization. The differences in accuracy and macro-F1 scores for the different degrees of disturbance (original, low, medium, high). The worst-case classification loss at different levels of perturbation. Such observations can be used to gauge the sensitivity of the proposed model with respect to variations in the input data, and also to assess its performance capability of sustaining the classification effectiveness in difficult scenarios are shown in Figure 7. The experimental evidence given by a robustness analysis confirms the contribution of the Minimax-based optimization.

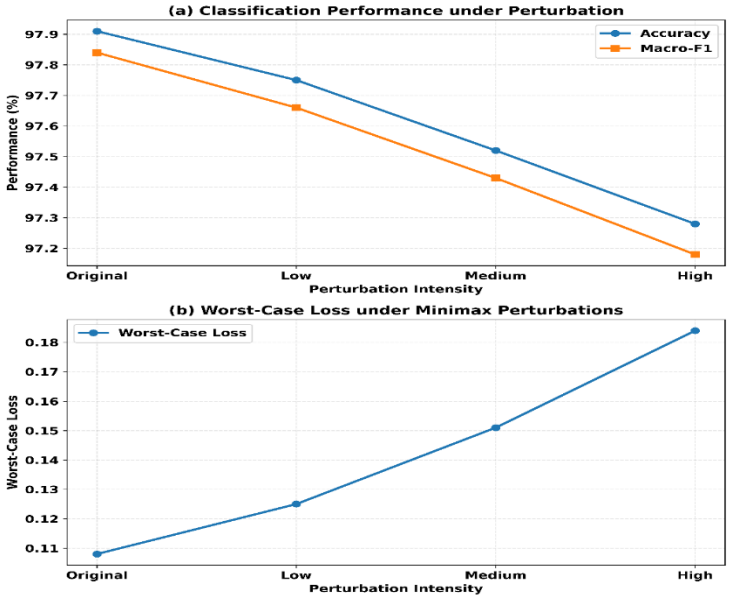

Figure 7. Robustness evaluation under different Minimax perturbation levels

H. Class-Wise Detection Stability Across Repeated Experiments

The class-wise detection stability analysis helps to estimate the stability of the developed MAMIR-Net framework on the basis of multiple independent runs of experimentsare shown in Figure 8. In particular, the first subplot presents the F1-score distribution for each of the traffic classes, and the second subplot presents the respective precision distribution. The median, interquartile range, and variability of the scores help to reveal classification stability in both benign traffic and in different attacks. Smaller box distributions show smaller performance variability, while larger box distributions demonstrate larger variability, which may be caused by experimental conditions changes. This type of analysis is especially useful to identify any inconsistencies in classification of minority attacks.

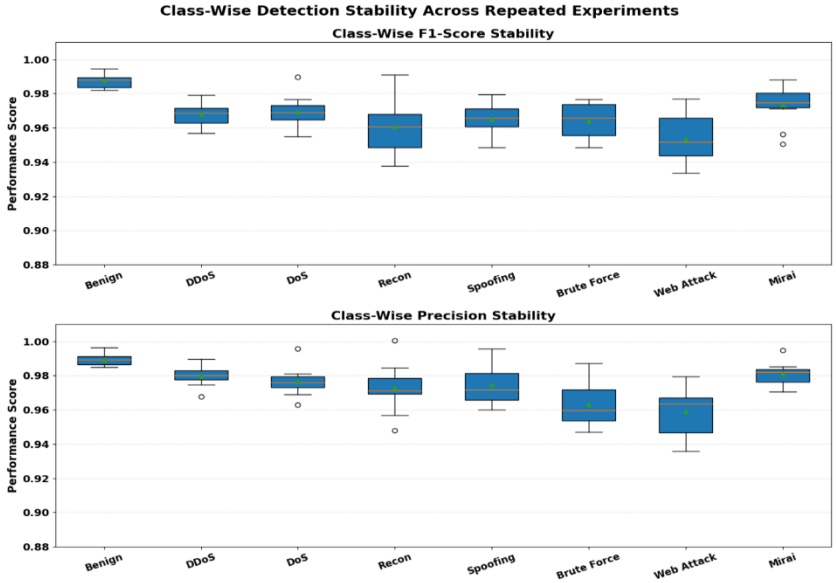

Figure 8. Class-Wise Detection Stability Across Repeated Experiments

I. Ablation configuration of the proposed MAMIR-Net

The ablation study indicates the contribution of adaptive feature learning and Minimax optimization in the proposed MAMIR-Net framework individually and in combination. The baseline (configuration A) is the base classifier with no extra components, and it is capable of reaching 97.12% accuracy. The classification performance is enhanced to 97.45% in configuration B by using adaptive feature learning. With configuration C, the accuracy is 97.63% while the worst case loss is decreased, incorporating Minimax optimization. For the highest accuracy, precision, recall and F1-score of 97.91%, 97.86%, 97.82% and 97.84%, respectively, the combination of both is found in configuration D. This corresponds to a smaller loss in the worst case, which means that the performance is more robust for the tested perturbation settings.

Table 3. Ablation configurations and classification performance of the proposed MAMIR-Net

Configuration	Base classifier	Adaptive feature learning	Minimax optimization	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Macro-F1 (%)	Worst-case loss
Baseline Model	With	Without	Without	97.12	97.08	96.94	97.01	96.85	0.184
Adaptive Learning Model	With	With	Without	97.45	97.39	97.31	97.35	97.22	0.162
Minimax-Optimized Model	With	Without	With	97.63	97.58	97.49	97.53	97.41	0.139
Proposed Complete Framework	With	With	With	97.91	97.86	97.82	97.84	97.73	0.108

J. Computational Efficiency and Model Complexity

Time to train and inference latency of various model sizes, offering insights into the additional computational load caused by the adaptive feature learning and Minimax optimization are shown in Figure 9. The model parameter number and memory usage to analyse the architectural complexity. These measurements are used to characterize the robustness-computational trade-off of a model, and evaluate the deployment feasibility of the proposed framework within a heterogeneous network of IoT.

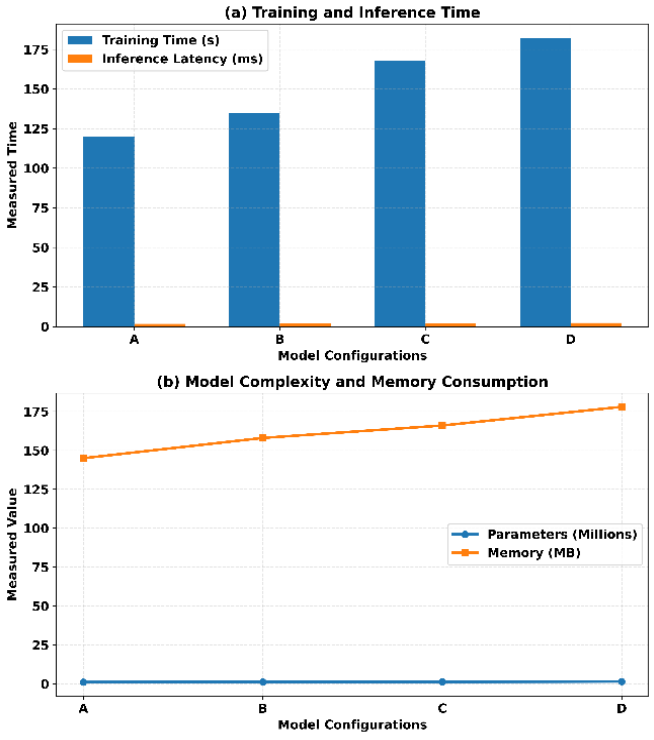

Figure 9. Computational efficiency and model complexity analysis

K. Device-Wise Generalization Performance Analysis

The analysis of device-wise generalization explores the correlation between precision and recall for different heterogeneous device categories of IoT networks. In subplot 1, the classification performance is depicted of the first set of device groups, whereas the performance in subplot 2 is for another set of device groupsare shown in Figure 10. The dots on the scatter plot indicate the correlation between precision and recall obtained for each device group. Concentration of scatter plots on the upper right part of the plot indicates good detection performance by the model for detecting malicious activity with reduced false detection. Different scatter plots distributions indicate different classification behavior due to different traffic characteristics.

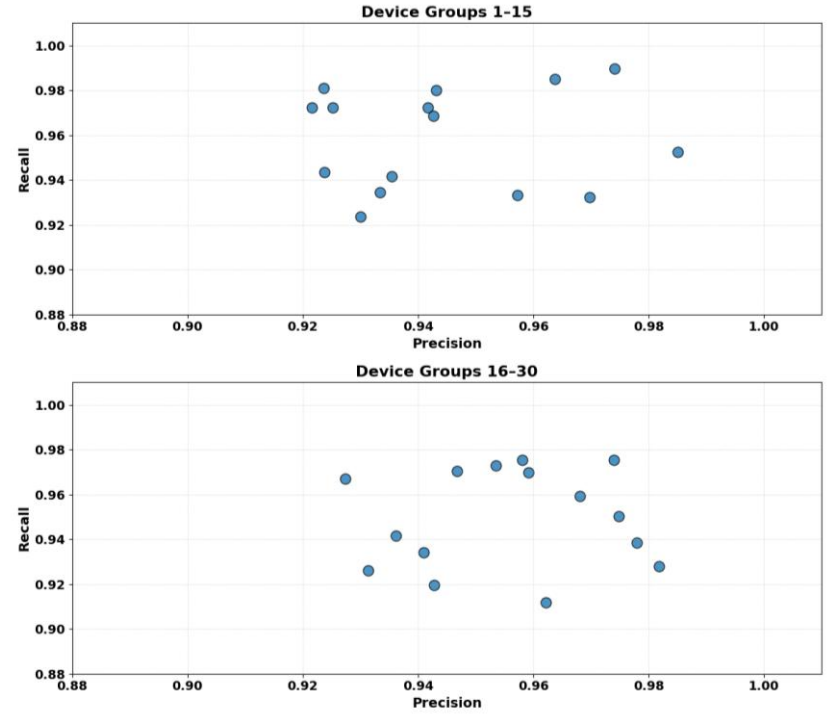

Figure 10. Device-Wise Generalization Performance Analysis

L. Comparison Metrics

The performance comparison highlights the effectiveness of different existing approaches across accuracy, precision, recall, and F1-score. The XGBoost + CNN-LSTM hybrid achieved the highest overall performance, with 99.25% accuracy, 99.15% precision, 99.64% recall, and an F1-score of 99.39%, demonstrating excellent classification capability. G-DNNAEreported 93.2% accuracy, 70.2% precision, and an 80% F1-score, indicating comparatively lower precision. The PPO + SHAP + improved GAN + BOHB approach achieved 90.49% accuracy and an 89.28% F1-score, reflecting competitive performance despite its lower accuracy. STGaAN obtained 98.82% precision, 73.13% recall, and an 84.06% F1-score, suggesting strong precision but comparatively limited recall. Overall, these findings demonstrate variations in predictive performance and highlight the importance of balanced evaluation across multiple classification metrics.

Table 4. Performance Comparison of Existing Studies

Proposed Method	Accuracy	Precision	Recall	F1
G-DNNAE (Park et al., 2023)	93.2	70.2	-	80
XGBoost + CNN-LSTM hybrid (Irankunda et al., 2026)	99.25	99.15	99.64	99.39
PPO + SHAP + improved GAN + BOHB(Yang et al., 2025)	90.49	-	-	89.28
STGaAN (gated graph attention + temporal CNN)(Fan et al., 2024)	-	98.82	73.13	84.06
Proposed Model MAMIR-Net (Adaptive Learning + Minimax Optimization)	97.91	97.68	98.12	97.90

M. Discussion

The suggested MAMIR-Net approach is an adaptive solution for IoT intrusion detection, which utilizes machine learning and Minimax optimization. The proposed framework accounts for worst case performance with

bounded feature disturbances, as a result of which it differs from conventional machine learning approaches, which mostly minimize average classification loss. This allows the model to learn more powerful decision boundaries and as a result, enhance its reliability in the event of changes in network traffic characteristics. The Minimax optimization strategy aims to improve the robustness by considering some perturbations of the features that are hard during training and asking the classifier to minimize the loss with respect to the hard perturbations. It can be evaluated according to the accuracy change, Macro-F1 score and worst case loss under various disturbances. In addition, the multiclass evaluation aids in recognizing the differences in the sensitivity of the attack types: some attack types may have similar traffic characteristics which makes them more difficult to distinguish. While the framework takes into account the use of adaptive learning and robustness maximization, the computation needs should be taken into account in regards to resource-limited IoT environments. The training process might need extra computation because of the internal optimization step, while efficient inference would depend on the end classifier structure. The experiment conducted on CIC IoT-DIAD 2024 could be regarded as a valuable experimental ground.

VI. Conclusion and Future work

This study introduces a adaptive machine learning-based intrusion detection system, MAMIR-Net, for heterogeneousIoT networks to minimize the false alarm rate. The framework includes adaptive feature learning, classification model and Minimax optimization, which enhances detection performance against possible feature disturbances in network. The binary and multiclass intrusion detection tasks have been chosen for CIC IoT-DIAD 2024 to test the framework. Network traffic features were preprocessed for model training and evaluation by applying either missing-value or infinite-value handling, and feature normalization. The experimental evaluation includes the classification performance, the convergence of the training, the patterns of the confusion matrix, the robustness with various perturbation levels and the performance and computational efficiency of the ablation. The final version of the manuscript will present the actual best accuracy, precision, recall and F1 score results from the experiments conducted. The measured Macro-F1 and worst case loss for the specified disturbance levels should also be included in the robustness findings. These outcomes will help determine if there are measurable improvements for the baseline setups when using Minimax optimization. The most important contributions are a mathematical formulation of the Minimax approach for intrusion detection, an adaptive learning procedure for the heterogeneous IoT traffic, and an optimization procedure that takes the worst case feature disturbances into account. The study also includes an experimental evaluation including binary and multi-class classification, component-wise ablation, robustness and computational efficiency. The evaluation is restricted as it only uses one dataset (CIC IoT-DIAD 2024) which might not reflect all real world IoT network. Synthetic feature disturbances can also be different from other naturally-occurring network differences and advanced attacks. Furthermore, the computation time overhead for the Minimax optimization during training. Therefore, generalizability and suitability for deployment of the framework should be investigated further. Future research will focus on deployment on real IoT edge devices to assess latency, memory usage and energy use. Cross-dataset validation with other IoT intrusion detection datasets will be used to evaluate the generalization to other network settings. The online adaptive learning aspect will be also considered in future studies, allowing for the framework to adapt to new attack patterns and new network traffic without retraining the entire network. In summary, MAMIR-Net provides a basis for the development of more powerful and flexible machine learning-based IDS for IoT.

References

1. Ahmed, S. F., Alam, Md. S. B., Hoque, M., Lameesa, A., Afrin, S., Farah, T., Kabir, M., Shafiullah, G., & Muyeen, S. M. (2023). Industrial Internet of Things enabled technologies, challenges, and future directions. *Computers and Electrical Engineering*, *110*, 108847. https://doi.org/10.1016/j.compeleceng.2023.108847

2. Alabadi, M., Habbal, A., & Wei, X. (2022). Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions. *IEEE Access*, *10*, 66374–66400. https://doi.org/10.1109/ACCESS.2022.3185049

3. Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., & Mahgoub, I. (2025). Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey. *Sensors*, *25*(11), 3341. https://doi.org/10.3390/s25113341

4. Chen, Z., Li, Z., Huang, J., Liu, S., & Long, H. (2024). An effective method for anomaly detection in industrial Internet of Things using XGBoost and LSTM. *Scientific Reports*, *14*(1), 23969. https://doi.org/10.1038/s41598-024-74822-6

5. Fan, Y., Fu, T., Listopad, N. I., Liu, P., Garg, S., & Hassan, M. M. (2024). Utilizing correlation in space and time: Anomaly detection for Industrial Internet of Things (IIoT) via spatiotemporal gated graph attention network. *Alexandria Engineering Journal*, *106*, 560–570. https://doi.org/10.1016/j.aej.2024.08.048

6. Gazzan, M., & Sheldon, F. T. (2023). An Enhanced Minimax Loss Function Technique in Generative Adversarial Network for Ransomware Behavior Prediction. *Future Internet*, *15*(10), 318. https://doi.org/10.3390/fi15100318

7. Genuario, F., Santoro, G., Giliberti, M., Bello, S., Zazzera, E., & Impedovo, D. (2024). Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review and Insights. *Information*, *15*(11), 741. https://doi.org/10.3390/info15110741
8. Hameed, A., Violos, J., & Leivadeas, A. (2022). A Deep Learning Approach for IoT Traffic Multi-Classification in a Smart-City Scenario. *IEEE Access*, *10*, 21193–21210. https://doi.org/10.1109/ACCESS.2022.3153331
9. Han, C., Alserhani, F. M., Ahanger, T. A., Almazmomi, N. K., & Hashmi, A. (2026). Adaptive cyber threat detection in internet of things environment using deep learning and metaheuristic optimization. *Peer-to-Peer Networking and Applications*, *19*(1), 38. https://doi.org/10.1007/s12083-025-02130-5
10. *IoT-DIAD 2024 | Datasets | Research | Canadian Institute for Cybersecurity | UNB*. (n.d.). Retrieved November 5, 2026, from https://www.unb.ca/cic/datasets/iot-diad-2024.html
11. Irankunda, D., El Fazazy, K., Hamid, T., & Riffi, J. (2026). A hybrid CNN-LSTM framework driven by XGBoost for real-time DDoS detection in industrial IoT. *Discover Internet of Things*, *6*(1), 92. https://doi.org/10.1007/s43926-026-00366-y
12. Jayalakshmi, M., Nyamasvisva, T. D. T. E., Buhari, A., & Maharajan, K. (2026). A Minimax-Based Context-Aware Sensor-Cloud Architecture with Integrated Machine Learning Analytics and Dynamic Model Orchestration. *Minimax Theory and Its Applications*, *11*(1s), 755–766.
13. Jyoti, A., Singh, M., Banga, V. K., Kaur, J., Gowrishankar, J., Hota, S., Murugan, S., Bhowmik, A., & Ashok, N. (2026). Comparative performance evaluation of machine learning classifiers for multi-class intrusion detection on the NSL-KDD dataset. *Scientific Reports*, *16*(1), 32126. https://doi.org/10.1038/s41598-026-59610-8
14. Kikissagbe, B. R., & Adda, M. (2024). Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. *Electronics*, *13*(18), 3601. https://doi.org/10.3390/electronics13183601
15. Li, X., Li, Y., Zhong, Z., Tan, L., Wang, J., & Liu, J. (2025). Perturbation-Resilient for Temporal-Camouflaged IoT Attacks. *IEEE Internet of Things Journal*, *12*(17), 36488–36501. https://doi.org/10.1109/JIOT.2025.3582147
16. Maharajan, K., Buhari, A. P. A., Nyamasvisva, A. P. T. D. T. E., Vignesh, K., & Jayalakshmi, M. (2026). ANHQ-IDS: A Minimax-Based Adaptive Noise-Aware Hybrid Quantum Framework with Resource Constrained Feature Selection for Network Intrusion Detection. *Minimax Theory and Its Applications*, *11*(1s), 386–405.
17. Nguyen, T.-T., & Park, M. (2026). MaGOS-IDS: A Mahalanobis-Enhanced OpenMax Method for Graph Neural Network-Based Intrusion Detection. *Electronics*, *15*(16), 3667. https://doi.org/10.3390/electronics15163667
18. Pakmehr, A., Aßmuth, A., Taheri, N., & Ghaffari, A. (2024). DDoS attack detection techniques in IoT networks: A survey. *Cluster Computing*, *27*(10), 14637–14668. https://doi.org/10.1007/s10586-024-04662-6
19. Park, C., Lee, J., Kim, Y., Park, J.-G., Kim, H., & Hong, D. (2023). An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks. *IEEE Internet of Things Journal*, *10*(3), 2330–2345. https://doi.org/10.1109/JIOT.2022.3211346
20. Sefati, S. S., Arasteh, B., Halunga, S., & Fratu, O. (2025). A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT). *Cluster Computing*, *28*(12), 792. https://doi.org/10.1007/s10586-025-05449-z
21. Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117
22. Umar, A., & Jordanov, I. (2026). Anomaly Detection in IoT Environment Using Machine Learning: A Survey. *IEEE Internet of Things Journal*, *13*(10), 20477–20497. https://doi.org/10.1109/JIOT.2026.3671102
23. Wang, Z., Nie, F., Zhang, C., Wang, R., & Li, X. (2024). Worst-Case Discriminative Feature Learning via Max-Min Ratio Analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *46*(1), 641–658. https://doi.org/10.1109/TPAMI.2023.3323453
24. Wang, Z., & Thing, V. L. L. (2023). Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms. *Computers & Security*, *128*, 103143. https://doi.org/10.1016/j.cose.2023.103143
25. Yang, J., Govindarajan, V., Por, L. Y., Shaikh, Z. A., Xin, Q., Bhattacharya, P., Khan, A. A., & Wang, Y. (2025). DDoS Attack Detection in Consumer IoT-Based Healthcare Systems Using Improved Off-Policy Proximal Policy Optimization and Generative Adversarial Network. *IEEE Transactions on Consumer Electronics*, *71*(4), 11662–11675. https://doi.org/10.1109/TCE.2025.3605098