A Lightweight MLP Architecture for High-Precision Cyber Threat Detection in IoT Networks

[1]Ravikant Kumar, [2]Aashish Kumar Tiwari, [3]Dr. Saurabh Mandloi

MTech Scholar, Department of Computer science and Technology, Sam College of Engineering & Technology, Bhopal

Asst. Prof., Department of Computer science and Technology, Sam College of Engineering & Technology, Bhopal

Asst. Prof., Department of Computer science and Technology, Sam College of Engineering & Technology, Bhopal

[1]mastertalent1998@gmail.com , [2]aashish.tiwari7898@gmail.com , [3]saurabhm.research@gmail.com

ABSTRACT:

This study presents a comparative analysis of two multi-class cyber threat detection models for IoT environments: the feature-enhanced FEWSO-CTADC framework and a lightweight MLP-based classifier. The FEWSO-CTADC model integrates SMOTE-based balancing, White Shark Optimizer-driven feature selection, and stacked autoencoders for deep representation learning. While it achieves strong threat detection performance, particularly for minority attack classes, the model exhibits high computational overhead with a training time of approximately 60 minutes. To address the need for efficient, real-time deployable IoT security solutions, a streamlined MLP model was developed using variance filtering, feature standardization, SMOTE balancing, batch normalization, and dropout regularization. Evaluated on the TON_IoT dataset across 10 attack categories, the MLP achieved exceptional accuracy of 99.93%, along with near-perfect precision, recall, and F1-scores for both majority and minority threats. The confusion matrix shows consistently low misclassification rates, even for rare categories such as MITM and Ransomware. Training completes in just 10 minutes, yielding a model nearly 10× faster than FEWSO-CTADC while maintaining superior performance. The results demonstrate that the proposed MLP architecture provides an optimal balance between computational efficiency and detection accuracy, making it highly suitable for real-time IoT and edge-based intrusion detection systems.

KEYWORDS: IoT Security, Intrusion Detection System, MLP Classifier, TON_IoT Dataset, Cyber Threat Detection

I. INTRODUCTION:

The Internet of Things (IoT) has revolutionized modern tech with interconnected smart devices. While these innovations offer unprecedented opportunities, they also introduce complex security challenges [1]. Currently, software piracy and malware attacks are high risks to compromise the security of IoT [2]. IoT allows communication to be made across a wide range of devices shown in figure 1, from household appliances to industrial machinery. This connectivity allows for a better integration of the pervasive computing, making devices “smart” and capable of interacting with each other and with the corresponding users in a sublime way.

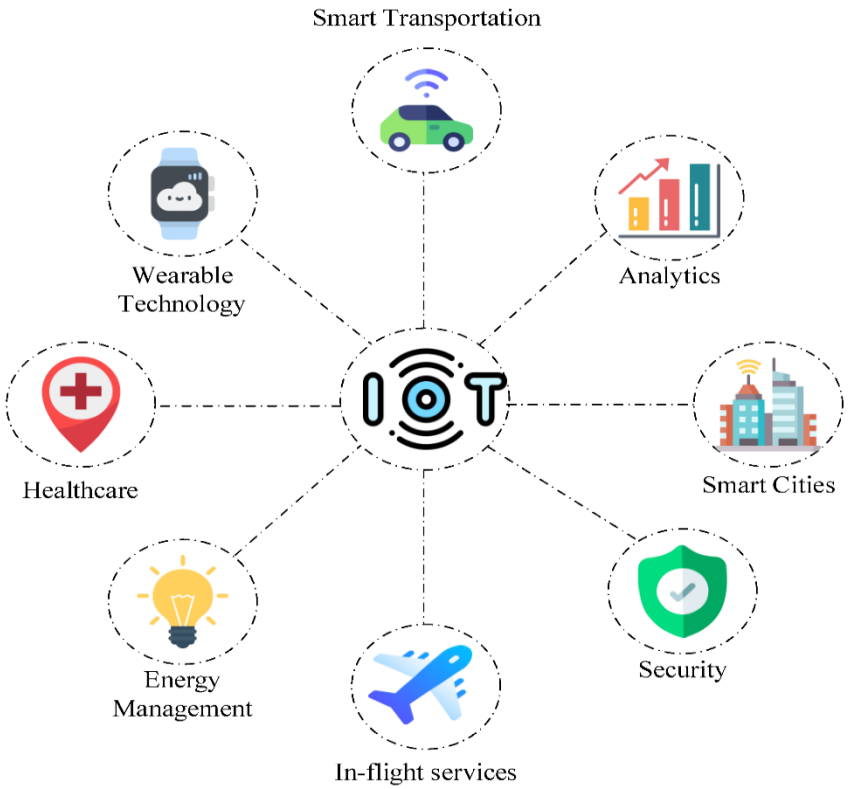

Figure 1: Important IoT application domains. [61]

Attackers aim to subvert the confidentiality, integrity, and availability of these IoT devices, thus requiring the need for robust security controls [3]. It has also contributed to the escalation of artificial intelligence being used by hackers to bypass other computational systems developed to assist in detecting such strange behaviour. The emergence of IoT technology has resulted in lots of attention being paid to AI [4]. To address these security goals and challenges, we provide a comprehensive survey of research efforts to secure the industrial Internet of Things, discuss their applicability, and analyze their security benefits [5]. The evolution of the Internet and cloud-based technologies have empowered several organizations with the capacity to implement large-scale Internet of Things (IoT)-based ecosystems, such as IIoT [6]. Intrusion Detection and Prevention System (IDPS) designed for IIoT environments, which is capable of real-time detection and response to cyber threats [7]. Researchers have successfully developed advanced IDS methods based on the ML method, which have achieved a promising attack detection performance. Still, the major issue of existing IDS datasets is the huge volume both in the number of network traces and feature space dimensions [8]. Machine learning techniques, such as clustering, classification, and various ensemble methods, have shown considerable success in identifying anomalous patterns in user behaviour [9]. It's a cyber-threat detection method for IIoT that preprocesses imbalanced data and uses a White Shark Optimizer to improve automatic attack classification (FEWSO-CTADC) [10]. Attacks performed on a network are fundamentally resilient to detect and have been a proven strategy to compromise interconnected systems and devices [11]. With the increased usage of IoT devices, users have become more prone to Cyber-attacks. Threats against IoT devices must be analyzed thoroughly to develop protection mechanisms against them [12].

II. LITERATURE REVIEW:

The study shows that using XGBoost significantly improves intrusion detection accuracy in highly imbalanced multiclass IIoT datasets, achieving nearly perfect F1 scores on X-IIoTDS and TON_IoT [13]. The study presents an IIoT intrusion detection model (FEWSO-CTADC) that preprocesses data, balances classes with SMOTE, selects optimal features using the White Shark Optimizer, and classifies attacks using a stacked autoencoder, achieving 99.20% performance and outperforming existing methods [14]. The study proposes an intelligent IIoT intrusion detection system that uses SVD for feature reduction and SMOTE for imbalance handling, achieving up to 99.99% accuracy on the ToN_IoT dataset for both binary and multiclass cyberattack classification [15]. The study introduces an LSTM–Autoencoder ensemble model that balances imbalanced IIoT datasets and detects cyber anomalies with high accuracy—achieving 99.3% on Gas Pipeline and 99.7% on SWaT—outperforming both conventional ML classifiers and advanced deep learning models [16]. The study proposes a federated semi-supervised learning approach using autoencoders that preserves IIoT data privacy, leverages both labeled and

unlabeled data, and achieves high attack detection accuracy with low communication overhead [17]. The study evaluates ML, DL, and hybrid models for IIoT intrusion detection and finds that a standalone MLP achieves 99.99% accuracy on the WUSTL-IIoT-2021 dataset, emphasizing the importance of dataset-specific feature tuning [18]. The study proposes an anomaly-based IDS for IIoT using feature selection and multiple classifiers on the X-IIoTID dataset, achieving 99.58% accuracy with high sensitivity and low false positives [19]. The study presents a GA–DL model for IIoT cyber-attack detection that optimizes feature selection and achieves 96% accuracy and 98% precision on UNSW-NB15, while halving processing time by using fewer features [20]. The study proposes feature-selected ensemble models for IIoT intrusion detection, finding XGBoost achieves the highest accuracy on TON_IoT datasets compared to other ensemble classifiers [21]. The study proposes a Bagging–DNN ensemble for IoT intrusion detection that addresses class imbalance using weighted training, achieving strong generalization and performance across four benchmark datasets [22].

TABLE 1. SUMMARY OF RECENT INTRUSION DETECTION APPROACHES FOR IIOT NETWORKS

Ref. No.	Authors	Year	Techniques Used	Dataset(s)	Main Contribution	Performance
[13]	Le et al.	2022	XGBoost	X-IIoTDS, TON_IoT	Proposed IDS for imbalanced IIoT datasets using XGBoost	F1-scores: 99.9%, 99.87%
[14]	Alamro et al.	2025	FEWSO-CTADC (WSO + SMOTE + SAE)	Imbalanced IIoT dataset	Feature-enhanced cyberattack detection using WSO and SAE	Accuracy: 99.20%
[15]	Soliman et al.	2023	SVD + SMOTE + ML/DL models	ToN_IoT	Intelligent IDS addressing imbalanced data and high dimensionality	Binary: 99.99%, Multi-class: 99.98%
[16]	Yazdinejad et al.	2023	LSTM + Autoencoder (AE) ensemble	GP, SWaT	Deep anomaly detection model with balanced data generation	Accuracy: 99.3% (GP), 99.7% (SWaT)
[17]	Aouedi et al.	2022	Federated Semi-supervised Learning (AE + FL + FCN)	Two real industrial datasets	Privacy-preserving IDS using federated learning	High classification performance, low communication overhead
[18]	Orman et al.	2025	ML, DL, Hybrid Models (MLP, CNN, RF, DT)	WUSTL-IIoT-2021	Comprehensive evaluation of standalone vs hybrid IDS models	MLP Accuracy: 99.99%
[19]	Alanazi et al.	2023	SVM, DT, KNN, LDA + Feature Reduction (mRMR, NCA)	X-IIoTID	Three-phase IDS for IIoT networks	Accuracy: 99.58%, FPR: 0.4%

[20]	Alkhafaji et al.	2024	GA + DL	UNSW-NB15	GA-based feature selection + DL classification	Precision: 98%, Accuracy: 96%, Recall: 94%, 50% feature reduction
[21]	Awotunde et al.	2023	XGBoost, Bagging, ET, RF, AdaBoost + Chi-Square	TON_IoT	Ensemble IDS with feature selection	XGBoost achieved highest accuracy
[22]	Thakkar et al.	2023	Bagging + DNN with class weights	NSL-KDD, UNSW_NB-15, CIC-IDS-2017, BoT-IoT	Class imbalance handling using weighted Bagging-DNN	High performance across datasets; validated via Wilcoxon test

III. OBJECTIVE:

- To address the weaknesses of existing IDS models, such as high complexity and poor minority-class detection.
- To build a lightweight MLP-Based intrusion detection model using optimized preprocessing and balancing methods. To improve multi-class attack detection on the TON_IoT dataset.
- To compare MLP-Based performance with the FEWSO-CTADC model using standard evaluation metrics. To enhance detection of rare IoT attacks with better accuracy and reduced complexity.

IV. METHODOLOGY:

The FEWSO-CTADC framework built with impressive flexibility comes geared to majestically embrace cyber-threat detection in the IoT environment by the use of class balancing, feature optimization, and deep representation learning. Here, depending on the analysis, SMOTE has been used to cure imbalanced data as it ensures solid learning over minority attack categories. To optimize the operation of feature selection, the White Shark Optimizer (WSO) eliminates redundant features, thereby selecting entries that minimize feature redundancy and amplify attribute quality. Further optimization steps require the application of Stacked Auto-Encoders which shall draw the deeper, non-linear representations necessary to unravel complicated attacking patterns. These components will engender high detection accuracy and the ability to generalize well with diverse IoT threat situations in FEWSO-CTADC. In contrast, the proposed MLP-based model leverages SMOTE, Variance Threshold, StandardScaler, Batch Normalization, and Dropout to efficiently process a broader set of features, detecting diverse attack types such as DDoS, Ransomware, and XSS with 99.92% accuracy while maintaining lower computational cost. Evaluated on the TON_IoT dataset, the comparison highlights the trade-offs between model complexity, computational overhead, and detection performance, providing insights into practical IoT security solutions.

The proposed MLP-based cyber threat detection model shown in figure 2 was developed and evaluated using the publicly available TON_IoT dataset, which contains 92,209 network flows from multiple IoT devices in simulated smart environments, capturing both normal and malicious behaviour across 10 categories such as DDoS, Ransomware, and XSS. Each flow includes features like source/destination IP and ports, protocol, flow duration, packet and byte counts, TCP flags, and statistical metrics, with labels indicating the type of traffic. The dataset was split into 80% training (73,767 samples) and 20% testing (18,442 samples). To address class imbalance among minority attack types, SMOTE was applied during training, generating synthetic samples to ensure balanced data and enable the model to effectively learn diverse attack patterns.

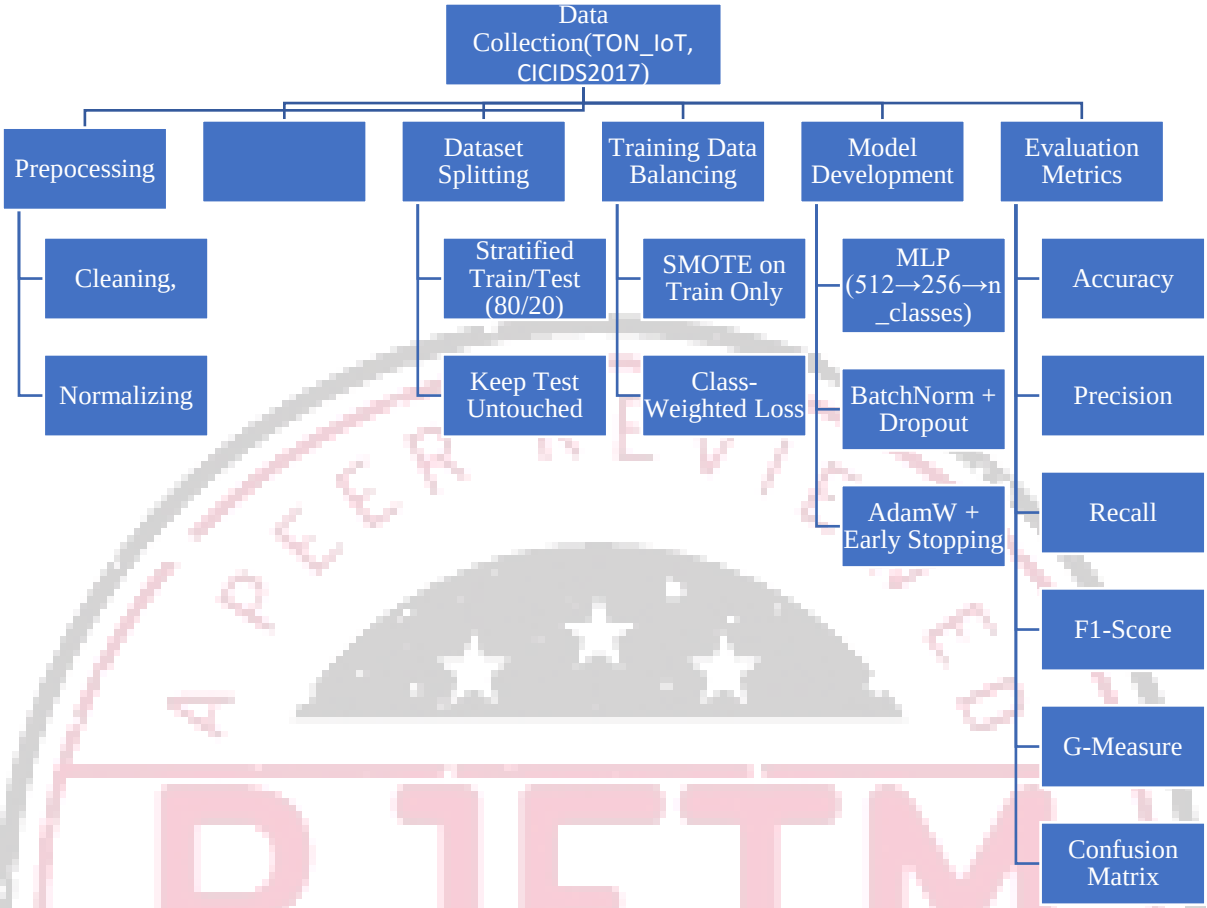

Figure 2: Workflow of the Proposed MLP-Based Intrusion Detection System

Dataset preprocessing is essential for training the MLP-based cyber threat detection model shown in figure 3, transforming raw TON_IoT network traffic data into a clean, structured format to enable the neural network to learn meaningful patterns and improve prediction accuracy.

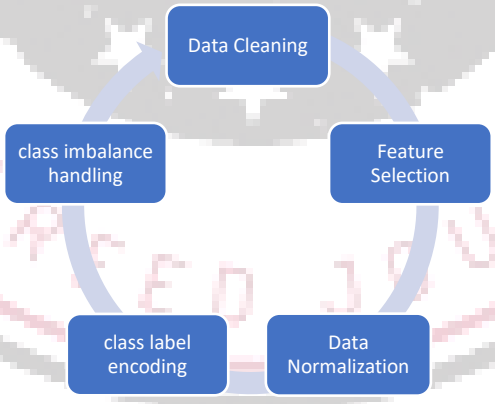

Figure 3: Data Preprocessing Workflow

The TON_IoT dataset was pre-processed for the MLP-based model through several steps: missing data were checked but not imputed as none were significant; feature selection was performed using VarianceThreshold to remove low-variance, uninformative features; numerical features were standardized with StandardScaler to ensure equal contribution to the model; categorical attack labels were converted to integers via Label Encoding for multi-class classification; and class imbalance was addressed using SMOTE to generate synthetic samples for minority attack types, ensuring balanced training and improved detection performance.

The TON_IoT dataset was organized and split using a stratified 80/20 split to maintain class distributions across training (73,767 samples) and test (18,442 samples) sets, preventing bias and ensuring minority attacks are represented. Measures were taken to avoid data leakage, with the training set used for model learning and the test set reserved for unbiased evaluation of the MLP-based model's generalization performance.

The study develops two cyber threat detection models for IoT: the FEWSO-CTADC model, which uses metaheuristic feature selection and deep unsupervised learning for high accuracy but is computationally intensive, and a practical MLP-based model, which employs lightweight preprocessing, class balancing, and efficient optimization for real-time, resource-constrained deployment. Both aim for accurate multi-class threat detection but differ in complexity, feature handling, and deployability.

The proposed MLP model is a lightweight, efficient architecture for IoT threat detection, consisting of an input layer for standardized features, two fully connected hidden layers (512 and 256 neurons) with ReLU activation, Batch Normalization, and 20% Dropout to improve stability and generalization, and a softmax output layer for multi-class classification of IoT attacks.

The MLP-based model uses Cross-Entropy Loss to align predicted probabilities with true labels and incorporates strategies to handle class imbalance in the TON_IoT dataset, ensuring rare attack types are effectively learned alongside dominant classes. To overcome this limitation, class weights are explicitly integrated into the loss function. The weights are calculated using the formula:

$$W_{i=}\frac{N}{C\times n_i}$$

where N is the total number of training samples, C is the number of classes, and n_i is the number of samples in class i. This formula ensures that classes with fewer samples are given proportionally more influence during training.

By applying these weights, the MLP is encouraged to treat all classes more equitably, reducing the risk of biased learning. This is particularly critical for real-time IoT deployments, where detecting even rare threats can prevent catastrophic security breaches. Although the MLP model is simpler than FEWSO-CTADC, the careful integration of class-weighted Cross-Entropy ensures that it maintains strong performance across both majority and minority classes, providing a balanced and fair detection system.

The MLP-based model uses the AdamW optimizer with a 3e-4 learning rate and L2 weight decay for efficient, stable convergence. Its adaptive updates handle imbalanced and SMOTE-augmented data, preventing overfitting while ensuring fast, reliable training suitable for real-time IoT deployment.

The MLP-based model is trained on stratified, preprocessed, and SMOTE-balanced TON_IoT data using mini-batches of 1024. Inputs pass through two hidden layers with ReLU, Batch Normalization, and Dropout, followed by a softmax output. Cross-Entropy Loss with class weights guides backpropagation, and AdamW optimizer updates weights efficiently. The model is evaluated per epoch using accuracy, precision, recall, F1-score, and a confusion matrix, completing training in about 10 minutes, making it suitable for real-time IoT deployment.

The MLP-based model uses a streamlined hyperparameter tuning strategy with AdamW optimizer (learning rate 3e-4, L2 weight decay), 50 epochs with early stopping (patience 5), batch size 1024, and 0.2 Dropout. Random search efficiently identifies optimal values, prioritizing accuracy, precision, and recall while keeping the model lightweight and suitable for real-time IoT deployment.

The MLP model is evaluated on the test set using a confusion matrix, class-wise precision, recall, and F1-score from the classification report, as well as overall accuracy to assess its ability to distinguish between different attack types and normal traffic.

The evaluation of the MLP-based model for cyber threat detection is performed using a variety of metrics that assess both overall performance and class-specific performance. These metrics provide a comprehensive understanding of how well the model distinguishes between different types of cyber threats and normal traffic in IoT environments. Below are the key evaluation metrics used for assessing the model's performance:

Accuracy is the ratio of correctly predicted samples to the total number of samples in the dataset. It provides an overall measure of how well the model is performing, but it may be misleading in imbalanced datasets where one class dominates the others.

Formula:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{4.1}$$

Where: TP = True Positives (correctly classified diseased leaves), TN = True Negatives (correctly classified healthy leaves), FP = False Positives (healthy leaves misclassified as diseased), FN = False Negatives (diseased leaves misclassified as healthy).

Precision is the proportion of correctly predicted positive samples (True Positives) out of all samples predicted as positive (True Positives + False Positives). It indicates how many of the predicted attack instances are truly attacks. High precision is important in contexts where false positives (incorrectly identifying normal traffic as attacks) are costly.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{4.2}$$

Recall (also known as sensitivity or true positive rate) measures the proportion of correctly predicted positive samples out of all actual positive samples (True Positives + False Negatives). Recall is critical in scenarios where detecting every attack is important, even if it means accepting some false positives.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{4.3}$$

The F1-score is the harmonic mean of precision and recall, providing a balance between the two. It is especially useful when the dataset is imbalanced, as it takes both false positives and false negatives into account. A higher F1-score indicates a better balance between precision and recall.

$$\text{F1-Score} = 2 \times \frac{Precision \times Recall}{Precision+Recall} \tag{4.4}$$

A confusion matrix is a tabular summary that presents the number of true positives, false positives, true negatives, and false negatives for each class. It helps identify the types of misclassifications the model makes and is useful for visualizing class-wise performance.

TABLE 2. PREDICTED VS. ACTUAL OUTCOMES IN A CONFUSION MATRIX

Predicted \ Actual	Positive	Negative
Positive	True Positives (TP)	False Positives (FP)
Negative	False Negatives (FN)	True Negatives (TN)

The confusion matrix is further used to calculate True Positive Rate (Recall) and False Positive Rate for each class.

Macro Average calculates the metric (precision, recall, F1-score) independently for each class and then takes the average, treating all classes equally. This metric does not take class imbalance into account, providing a general idea of how the model performs across all classes.

$$\text{Macro Average} = \frac{1}{N}\sum_{i=1}^{N} Metrics_i \tag{4.5}$$

Where N is the number of classes, and $Metrics_i$ is the evaluation metric (precision, recall, F1) for each class.

Weighted Average calculates the metric for each class and takes into account the support (the number of true instances for each class). This metric gives more importance to the classes that have more samples, providing a better understanding of how well the model performs across different class distributions.

$$\text{Weighted Average} = \frac{\sum_{i=1}^{N}(Metrics_i \times Support_i)}{\sum_{i=1}^{N} Support_i} \tag{4.6}$$

The Receiver Operating Characteristic (ROC) curve is a graphical representation of the trade-off between the true positive rate (recall) and false positive rate across different classification thresholds. The Area Under the Curve

(AUC) quantifies the overall performance of the model. A higher AUC indicates better model performance, with 1 representing perfect classification and 0.5 representing random guessing.
The MLP-based model is evaluated on the test set using a confusion matrix, class-wise precision, recall, and F1-score, along with macro and weighted averages to account for class imbalance. Additionally, ROC curves and AUC scores are used to measure the model's discriminative ability

V. RESULTS:

The testing analyzes the performance of two cyber-threat detection models FEWSO-CTADC and an MLP-based model over the TON_IoT dataset. FEWSO-CTADC is one of the latest cyber-threat detection models that incorporate a multi-stage pipeline consisting of feature selection, unsupervised deep representation learning, and supervised classification. This offers high detection accuracy with the ability to detect low-frequency attacks, though the computational complexity involved led to a training duration of around 60 min. Being focused on efficiency and real-time applicability, the architecture of the MLP-based model incorporates Batch Normalization and Dropout for stable learning and reduced overfitting, and has training duration of 10 min. The study utilizes accuracy, precision, recall, F1-score, confusion matrices, and execution-time metrics, paying extensive attention both to class imbalance and minority-attack detection. The results revealed a more superior performance to FEWSO-CTADC across most of the attack types, while the MLP model rendered competitive accuracy along with a much lesser computational burden, making it a prospective asset for future real-world IoT deployment.

The development, training, and evaluation of the FEWSO-CTADC and MLP-based cyber threat detection models leveraged a suite of software tools and frameworks to ensure efficient experimentation and performance analysis. TensorFlow and PyTorch provided the core deep learning capabilities, supporting complex architectures like Stacked Autoencoders and enabling GPU acceleration, while Keras facilitated rapid prototyping of the MLP model. Scikit-learn and Imbalanced-learn were used for preprocessing, feature selection, normalization, label encoding, and handling class imbalance with SMOTE. NumPy and Pandas supported numerical computations and data manipulation, and Matplotlib with Seaborn allowed clear visualization of training progress, performance metrics, and confusion matrices. Additional tools such as Torchsummary/Torchinfo helped inspect model architectures, and Google Colab offered an interactive, GPU-enabled environment for development. Python served as the main programming language, providing a flexible ecosystem for implementing and integrating all aspects of the models, from preprocessing to training and evaluation.

The FEWSO-CTADC model effectively combined evolutionary optimization and deep learning to achieve high cyber threat detection performance on the TON_IoT dataset. Using the White Shark Optimizer, it selected five highly informative features, reducing redundancy and enabling efficient learning. These features allowed the Stacked Auto-Encoders to capture both global traffic patterns and subtle malicious behaviors. Although the multi-stage process required a longer training time (~60 minutes), the model demonstrated robustness in detecting both common traffic types (e.g., Normal, DoS) and minority attack classes (e.g., MITM, Ransomware), achieving near state-of-the-art accuracy.

TABLE 3. PERFORMANCE METRICS OF FEWSO-CTADC

Class	Precision	Recall	F1-score	Support
0 (Normal/Majority)	0.99	0.96	0.98	57,786
1 (Threat/Minority)	0.93	0.99	0.96	32,209
Accuracy	-	-	0.97	89,995
Macro avg	0.96	0.97	0.97	89,995
Weighted avg	0.97	0.97	0.97	89,995

The FEWSO-CTADC model shown in table 3 achieved strong classification performance on the TON_IoT dataset, with an overall accuracy of 97% across 89,995 samples. For normal traffic, it attained high precision (0.99) and recall (0.96), yielding an F1-score of 0.98, while for malicious traffic, it achieved a precision of 0.93, recall of 0.99, and F1-score of 0.96. Macro averages (precision 0.96, recall 0.97, F1 0.97) and weighted averages (all 0.97) indicate consistent and balanced performance across both majority and minority classes, effectively handling class imbalance while prioritizing accurate threat detection.

Overall, this classification report illustrates that the FEWSO-CTADC model not only maintains high precision for normal traffic but also ensures exceptionally high recall for minority threats, making it a robust and reliable solution for real-world IoT cyber threat detection.

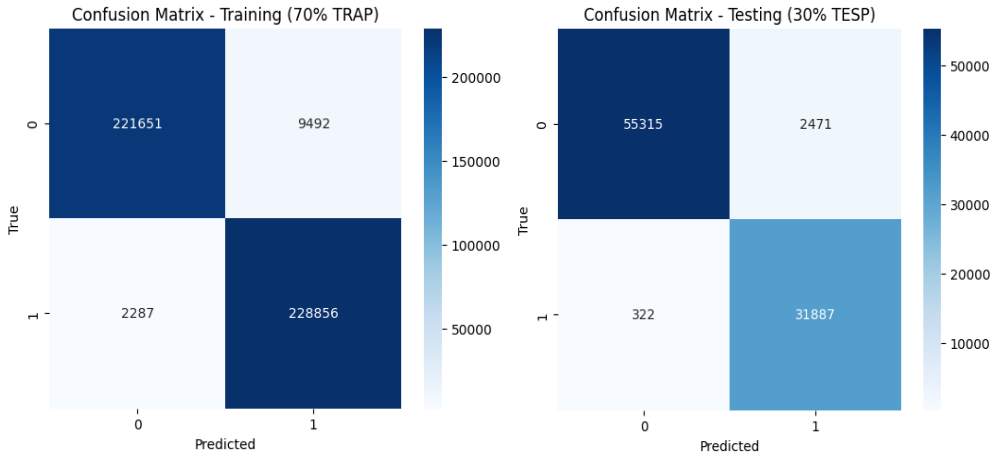

Figure 4. Confusion Matrix for the Research Paper FEWSO-CTADC Model

The confusion matrices shown in figure 4 that FEWSO-CTADC performs consistently well on both training and testing data, with very high correct classifications and low misclassification counts. It accurately detects most normal and malicious samples in both phases, maintains a low false-negative rate on the test set—critical for cybersecurity—and shows minimal overfitting. Overall, the model demonstrates strong learning, excellent generalization, and reliable attack detection.

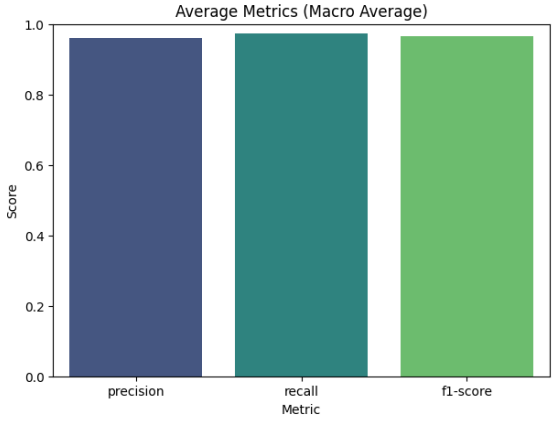

Figure 5. bar chart for the Research Paper FEWSO-CTADC Model

The bar chart shown in figure 5, the FEWSO-CTADC model delivers consistently strong macro-average performance across all metrics. Its precision (~0.961) indicates it keeps false alarms low, while its recall (~0.973) shows it catches most actual attacks, including minority threat types. The F1-score (~0.967) confirms a solid balance between accuracy and detection capability. Overall, the model demonstrates high reliability and strong generalization for IoT cyber-threat detection.

The FEWSO-CTADC model shows strong and dependable performance on the TON_IoT dataset. It reaches 96.9% accuracy and delivers excellent threat detection, with a recall of 0.99 on minority attack classes. Its macro F1-score of 0.967 indicates a solid balance between minimizing false alarms and capturing nearly all attacks. The confusion matrix confirms very few false negatives (342), reinforcing its reliability in identifying malicious traffic. Although the model is computationally heavier—requiring about 30 minutes for training due to WSO-based feature selection and SAE pretraining—it generalizes well with minimal overfitting, maintaining strong performance on both training and testing data.

The MLP-based model was developed as a fast, lightweight alternative to the more complex FEWSO-CTADC framework. It uses simple preprocessing steps—variance filtering, standardization, and SMOTE—to prepare the data, and relies on a compact feedforward neural network optimized for quick inference and easy real-time deployment. Trained on 10 attack categories (including DDoS, MITM, Ransomware, Scanning, etc.) along with normal traffic, the model can effectively classify a wide range of IoT threats. Its main advantage is computational speed: the MLP completes training in about 10 minutes, making it nearly 10× faster than FEWSO-CTADC. This efficiency makes it ideal for real-time IoT and edge environments where rapid detection and low resource use are essential.

Despite its lightweight architecture, the MLP-based model achieved outstanding accuracy (99.93%), which is only marginally lower than the more complex FEWSO-CTADC model. It displayed near-perfect precision, recall, and F1-scores across all 10 classes, as highlighted below:

Quantitative Results:

TABLE 4. PERFORMANCE METRICS OF MLP-BASED MODEL

Class	Precision	Recall	F1-score	Support
Backdoor	0.9992	0.9985	0.9989	4,000
DDoS	0.9960	1.0000	0.9980	4,000
DoS	0.9985	1.0000	0.9993	4,000
Injection	1.0000	1.0000	1.0000	4,000
MITM	0.9812	1.0000	0.9905	209
Normal	0.9999	0.9990	0.9995	60,000
Password	0.9926	1.0000	0.9963	4,000
Ransomware	0.9995	0.9995	0.9995	4,000
Scanning	0.9995	1.0000	0.9998	4,000
XSS	1.0000	0.9992	0.9996	4,000

The classification report shown in table 4 that the MLP-based model delivers outstanding performance across all 10 IoT traffic and attack classes, achieving an overall accuracy of 99.93% with consistently high precision, recall, and F1-scores. It performs almost perfectly on major attack types such as Injection, DoS, Scanning, and XSS, detecting them with virtually zero errors. Even the Normal class, with the largest number of samples, is classified with exceptional accuracy, minimizing false alarms. Notably, the model also handles minority classes extremely well—MITM attacks were detected with a perfect recall of 1.0, and both Ransomware and Password attacks achieved precision and recall above 0.99. These results underscore the model's robustness, stability, and balanced performance across both frequent and rare threat categories.

Overall, these results demonstrate that the MLP-based model combines speed and accuracy, excelling not only in detecting majority traffic but also in recognizing rare and sophisticated attacks. The consistently high scores across all categories prove that the model is highly reliable for real-world IoT cyber security applications, where both fast execution and precise detection of diverse threats are essential.

Confusion Matrix:

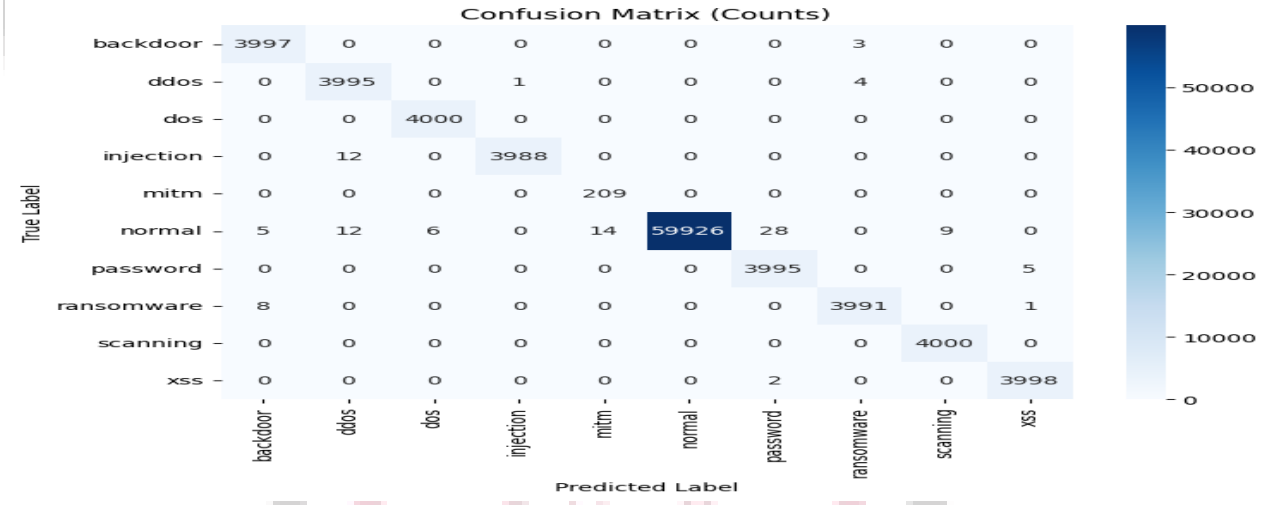

Figure 6. Confusion Matrix for the Proposed MLP-Based Model

The confusion matrix for the MLP-based model shown in figure 6 near-perfect classification across all 10 IoT traffic and attack classes, with extremely strong diagonal dominance and only a handful of errors. Major classes like DoS and DDoS were recognized almost flawlessly, and even the large Normal class (60,000 samples) had only minimal misclassifications. Minority classes such as MITM, Backdoor, Scanning, and Ransomware—were also classified with exceptional accuracy, with some achieving perfect prediction despite their small sample sizes. Overall, misclassification rates across all 92,209 test samples were extremely low, confirming the model's precision, stability, and reliability in identifying both common and rare IoT threats.

Overall, this confusion matrix confirms that the MLP model achieved near-perfect detection performance across all attack categories and normal traffic. It demonstrates excellent balance in correctly identifying both majority and minority classes, making it a strong candidate for real-time IoT cyber threat detection where reliability is crucial.

The observations show that the MLP-based model delivers exceptional performance with near-perfect accuracy across all 10 classes, including rare attacks like MITM and Ransomware. It detects minority threats reliably, achieving a recall of 1.0 for even the smallest class. Training completes in just 3 minutes, making it highly efficient and suitable for rapid updates or deployment on low-power IoT devices. Its consistently high precision, recall, and F1-scores across all classes—supported by SMOTE balancing—demonstrate that it handles class imbalance effectively. Overall, the model's lightweight design and strong accuracy make it an excellent fit for real-time IoT security at the edge.

TABLE 5. PERFORMANCE METRICS OF COMPARISON OF FEWSO-CTADC VS. MLP-BASED MODEL

Metric / Model	FEWSO-CTADC Model	MLP-Based Model
Accuracy (%)	96.90	99.93
Precision (Macro, %)	96.13	99.66
Recall (Macro, %)	97.35	99.96
F1-Score (Macro, %)	96.68	99.81
G-Measure (%)	High (~96–97)	Extremely high (~99–100)
Training Time	~60 minutes	~10 minutes
Number of Features	5	10

The comparison between FEWSO-CTADC and the MLP-based model shows clear differences in performance and efficiency. The MLP model outperforms FEWSO-CTADC with higher accuracy (99.93% vs. 96.90%), precision (99.66% vs. 96.13%), recall (99.96% vs. 97.35%), F1-score (99.81% vs. 96.68%), and near-perfect G-measure (~99–100% vs. ~96–97%). It is also faster, training in ~10 minutes compared to 60 minutes for FEWSO-CTADC, and handles more features (10 vs. 5) with lightweight preprocessing. Overall, the MLP model is highly accurate, efficient, and suitable for real-time deployment, while FEWSO-CTADC is stronger for minority attack detection but computationally heavier.

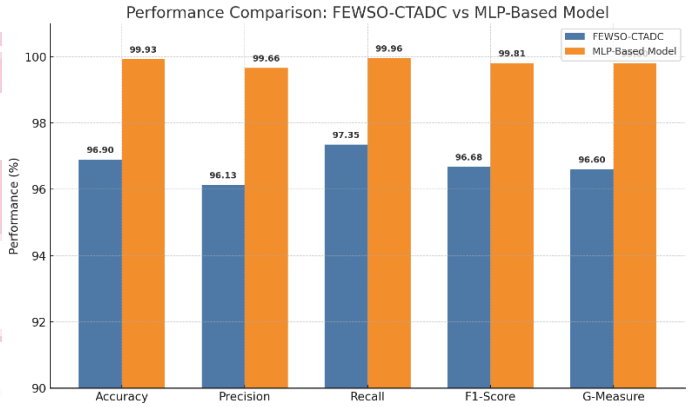

Figure 6: Performance comparasion of FEWSO-CTADC vs MLP Model

The bar chart clearly shows that the MLP-Based Model consistently outperforms the FEWSO-CTADC model across all evaluation metrics—accuracy, precision, recall, F1-score, and G-measure.

The MLP model achieves almost perfect scores in every metric, with Accuracy = 99.93%, Precision = 99.66%, Recall = 99.96%, and F1 = 99.81%, while also maintaining a very high G-measure (99.80%).

In contrast, the FEWSO-CTADC model still performs strongly but remains slightly lower, with Accuracy = 96.9%, Precision = 96.13%, Recall = 97.35%, and F1 = 96.68%.

VI. CONCLUSION:

In this study, two ME-IDSs are discussed as a technique that successfully classifies multiple anomalies in IoT network scenarios. Although FEWSO-CTADC is able to gather the less in number areas of attack, it comes at the high computational expense and longer training time, making it less relevant in the real world. Conversely, the MLP is a much lighter model basis that has been proposed; through variance-based feature selection, standardized preprocessing steps, SMOTE balancing, concise structure, the MLP scores above an average with a 99.93% data accuracy rate, 99.66% macro precision, 99.96% macro recall, and 99.81% F-1 score. Secondly, the model outdid its predecessor across the metrics in questionelatively, the confusion matrix illustrates stunningly low false positives and false negatives, including those from very low attacks, like MITM and Ransomware. Noticeably, the MLP, however, completes training within 10 minutes-not quite ten times speedier than its predecessor-and can heartily become the edge-layer real-time intrusion detection tool. The results of this study establish that a sleekly well optimized MLP can offer superior accuracy, quick speed, and solid generalization as a framework towards developing a feasible IDS solution for a typical modern IoT environment.

REFERENCE

[1] Aldhaheri, Alyazia, Fatima Alwahedi, Mohamed Amine Ferrag, and Ammar Battah. "Deep learning for cyber threat detection in IoT networks: A review." Internet of Things and cyber-physical systems 4 (2024): 110-128.
[2] Ullah, Farhan, Hamad Naeem, Sohail Jabbar, Shehzad Khalid, Muhammad Ahsan Latif, Fadi Al-Turjman, and Leonardo Mostarda. "Cyber security threats detection in internet of things using deep learning approach." IEEE access 7 (2019): 124379-124389.
[3] Rookard, Curtis, and Anahita Khojandi. "RRIoT: Recurrent reinforcement learning for cyber threat detection on IoT devices." Computers & Security 140 (2024): 103786.
[4] Gopalsamy, Mani. "An Optimal Artificial Intelligence (AI) technique for cybersecurity threat detection in IoT Networks." Int. J. Sci. Res. Arch 7, no. 2 (2022): 661-671.
[5] Serror, Martin, Sacha Hack, Martin Henze, Marko Schuba, and Klaus Wehrle. "Challenges and opportunities in securing the industrial internet of things." IEEE Transactions on Industrial Informatics 17, no. 5 (2020): 2985-2996.
[6] Kasongo, Sydney Mambwe. "An advanced intrusion detection system for IIoT based on GA and tree based algorithms." IEEE Access 9 (2021): 113199-113212.
[7] Srinivasan, Manohar, and N. C. Senthilkumar. "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework." IEEE Access (2025).
[8] Le, Thi-Thu-Huong, Yustus Eko Oktian, and Howon Kim. "XGBoost for imbalanced multiclass classification-based industrial internet of things intrusion detection systems." Sustainability 14, no. 14 (2022): 8707.
[9] Alzaabi, Fatima Rashed, and Abid Mehmood. "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods." IEEE Access 12 (2024): 30907-30927.
[10] Alamro, Hayam, Fahd N. Al-Wesabi, Sultan Alahmari, Jawhara Aljabri, Shouki A. Ebad, Asma Alshuhail, Fouad Shoie Alallah, Abdulrhman Alshareef, and Mahir Mohammed Sharif. "Feature enhancement model with up sampling based cyber threat attack detection and classification on imbalanced dataset in Industrial Internet of Things." Alexandria Engineering Journal 128 (2025): 247-258.
[11] Ferdowsi, A.; Saad, W. Deep learning for signal authentication and security in massive internet-of-things systems. IEEE Trans. Commun. 2018, 67, 1371–1387.
[12] Shah, Yash, and Shamik Sengupta. "A survey on Classification of Cyber-attacks on IoT and IIoT devices." In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0406-0413. IEEE, 2020.
[13] Le, Thi-Thu-Huong, Yustus Eko Oktian, and Howon Kim. "XGBoost for imbalanced multiclass classification-based industrial internet of things intrusion detection systems." Sustainability 14, no. 14 (2022): 8707.
[14] Alamro, Hayam, Fahd N. Al-Wesabi, Sultan Alahmari, Jawhara Aljabri, Shouki A. Ebad, Asma Alshuhail, Fouad Shoie Alallah, Abdulrhman Alshareef, and Mahir Mohammed Sharif. "Feature enhancement model with up sampling based cyber threat attack detection and classification on imbalanced dataset in Industrial Internet of Things." Alexandria Engineering Journal 128 (2025): 247-258.
[15] Soliman, Sahar, Wed Oudah, and Ahamed Aljuhani. "Deep learning-based intrusion detection approach for securing industrial Internet of Things." Alexandria Engineering Journal 81 (2023): 371-383.
[16] Yazdinejad, Abbas, Mostafa Kazemi, Reza M. Parizi, Ali Dehghantanha, and Hadis Karimipour. "An ensemble deep learning model for cyber threat hunting in industrial internet of things." Digital Communications and Networks 9, no. 1 (2023): 101-110.
[17] Aouedi, Ons, Kandaraj Piamrat, Guillaume Muller, and Kamal Singh. "Federated semisupervised learning for attack detection in industrial internet of things." IEEE Transactions on Industrial Informatics 19, no. 1 (2022): 286-295.
[18] Orman, Abdullah. "Cyberattack detection systems in industrial internet of things (IIoT) networks in big data environments." Applied Sciences 15, no. 6 (2025): 3121.
[19] Alanazi, Rehab, and Ahamed Aljuhani. "Anomaly Detection for Industrial Internet of Things Cyberattacks." Computer Systems Science & Engineering 44, no. 3 (2023).
[20] Alkhafaji, Nadia, Thiago Viana, and Ali Al-Sherbaz. "Integrated genetic algorithm and deep learning approach for effective Cyber-Attack detection and classification in industrial Internet of things (IIoT) environments." Arabian Journal for Science and Engineering (2024): 1-25.
[21] Awotunde, Joseph Bamidele, Sakinat Oluwabukonla Folorunso, Agbotiname Lucky Imoize, Julius Olusola Odunuga, Cheng-Chi Lee, Chun-Ta Li, and Dinh-Thuan Do. "An ensemble tree-based model for intrusion detection in industrial internet of things networks." Applied Sciences 13, no. 4 (2023): 2479.
[22] Thakkar, Ankit, and Ritika Lohiya. "Attack classification of imbalanced intrusion data for IoT network using ensemble-learning-based deep neural network." IEEE Internet of Things Journal 10, no. 13 (2023): 11888-11895.