European Journal of Clinical Pharmacy

Print ISSN: 2385-409X **Online ISSN**: 3105-0409

Website: https://farmclin.com/

Original Research Article

Multi-Layer Perceptron-Based Intrusion Detection For Reliable IoT Security

Article History:

Name of Author:

Azharudin Ansari[1], Dr. Kamlesh Gupta[2], Joy Bhattacharjee[3]

Affiliation: 1*M.Tech Scholar,Department of Computer Science & Engineering Technocrats Institute Of Technology Bhopal, India.*

2Department of Computer Science & Engineering Technocrats Institute Of Technology Bhopal, India

3Department of Computer Science & Engineering Technocrats Institute Of Technology Bhopal, India

Received*:* 05-11-2025

Revised*:* 20-11-2025

Accepted*:* 16-12-2025

Published*:* 30-12-2025

Abstract: IoT environments generate massive, heterogeneous network traffic that is increasingly targeted by sophisticated cyberattacks, demanding detection models that are both accurate and computationally efficient. This work evaluates two contrasting deep-learning approaches—FEWSO-CTADC, a hybrid model combining White Shark Optimizer–based feature selection with Stacked Auto-Encoders, and a lightweight Multi-Layer Perceptron (MLP) model—using the TON_IoT dataset. FEWSO-CTADC leverages evolutionary optimization and unsupervised representation learning to extract five optimized features, achieving strong performance across normal and minority attack classes with 96.9% accuracy. However, its multi-stage training pipeline requires significant computational time (~60 minutes). In contrast, the proposed MLP model uses 10 key features, SMOTE balancing, and minimal preprocessing, reducing training time to ~10 minutes while achieving near-perfect performance. The MLP obtained 99.93% accuracy, 99.66% precision, 99.96% recall, and 99.81% F1-score, outperforming FEWSO-CTADC across all metrics. Confusion-matrix analysis further confirmed exceptionally low misclassification rates, even for rare attacks such as MITM, Password, and Ransomware. The results demonstrate that while FEWSO-CTADC remains strong for feature-optimized offline analysis, the MLP model is more suitable for real-time IoT deployments due to its high accuracy, speed, and low computational cost. Overall, the study provides a clear benchmark comparison, highlighting the practicality of lightweight neural architectures for modern IoT security.

Keywords: IoT Cyber Threat Detection, MLP Classifier, FEWSO-CTADC, TON_IoT Dataset, Intrusion Detection Systems

INTRODUCTION

In industries, where machines and processes are interconnected by sensors and data analytics for real-time monitoring and automation, the term IIoT is in use. But increased connectivity brings with it emerging cyber-security risks [1]. IIoT links industrial machines, sensors, and control systems through connected computing technologies to improve decisions and efficiency across sectors like manufacturing, energy, transport, and healthcare. [2].

IIoT relies on massive real-time data flows from industrial devices to central or cloud systems, enabling intelligent automation, predictive maintenance, and better decision-making [3].

Industrial systems are increasingly hit by attacks like DDoS, spoofing, and ransomware, but traditional IT security tools fail in IIoT due to limited resources, diverse devices, and strict real-time requirements [4].

Fig. 1. Unveiling Cyber Threats in Industry IoT

With the wide network connection involved in an Industry Internet of Things, threats to cyber security are a huge concern. The perpetrator may have access to communication links, sensors, or control systems and either cause disruption to the industrial operations or steal sensitive data. To have systems in place for detection and mitigation, described in figure 1, it is necessary to understand the various types of attacks, entry points for attacks, and how they might affect industrial operations [5].

Cyberattacks on IIoT networks may severely paralyse industrial processes and endanger safety. Successful attacks may cause production shutdowns or, perhaps, malfunc-tion of equipment, together with the violation of very critical data, thereby affecting productivity and revenue directly [6].

Feature engineering boosts IIoT threat-detection accuracy by extracting the most informative, non-redundant attributes from large, diverse network data to better identify attacks [7]. It also creates new, compact variables from high-dimensional and noisy IIoT data so detection models focus on meaningful attack patterns rather than irrelevant noise [8].

Classification algorithms are critical to the detection and classification of cyber threats for Industrial Internet of Things networks [9].

With the sharp and quick advent of numerous Industrial Internet of Things (IIoT) technologies, there has been a noticeable increase in automation, efficiency, and real-time monitoring of industrial systems [10]. However, the scarcity of secure connectivity means industrial operations are targeted by various cyber threats, including data injection, spoofing, or DoS (denial of service), which disrupt existing operations to gain monetary benefits, sometimes risking safety hazards. Detection of such threats gets even more critical since the imbalance in IIoT datasets is a given condition-Attack instances are overwhelmingly fewer than normal traffic, so any conventional machine learning model becomes biased against attack detection-functioning poorly [11].

I. LITERATURE REVIEW

They proposed a multi-stage feature-selection plus LLM-augmented IDS using federated LightGBM that achieved strong metrics but struggled on highly imbalanced or noisy datasets [12]. They used TGAN-based deep learning for synthetic data generation, reaching high accuracy but becoming too computationally heavy for resource-limited IoT devices [13]. They evaluated multiple feature-selection approaches that improved detection performance, though results varied depending on network topology and dataset traits [14]. They applied data-augmentation-enhanced deep learning with strong accuracy and AUC but depended heavily on large labeled datasets rarely available in real IoT environments [15]. Built a hybrid deep-learning IDS with optimized feature selection achieving strong scores but sensitive to the quality and relevance of selected features across applications [16]. They introduced a gradient-scoring-based feature selection method improving efficiency and accuracy but inconsistent across different IoT device configurations [17].

They developed a lightweight aggregation-based IDS that delivered high performance yet added latency due to extra aggregation overhead [18]. They proposed a feature-engineering method using mean-decrease accuracy and exponential decay that improved F1 and training time but was highly noise-sensitive [19]. Study created an unsupervised domain-adaptation IDS that boosted accuracy by 16.9% but relied heavily on high-quality source domain data [20]. They designed an adaptive self-improving domain-adaptation model with strong precision and recall but required prohibitively expensive training resources [21].

TABLE I. COMPARATIVE ANALYSIS OF RECENT IOT/IIOT INTRUSION DETECTION METHODS AND THEIR PERFORMANCE

Ref	Method / Model	Key Idea	Accuracy	Other Performance Metrics	Limitation
[12]	Multi-stage feature selection + LLM-based augmentation + FL-LightGBM	MCP-based feature selection with LLM-generated data in federated learning	**98.6%**	Precision 97.8%, Recall 98.2%, F1 98.0%, AUC 0.991	Underperforms on highly imbalanced or noisy datasets
[13]	Deep Learning IDS + TGAN	GAN-based synthetic augmentation for tabular IoT data	**96.7%**	Precision 95.4%, Recall 96.1%, F1 95.7%, AUC 0.985	Computationally heavy; unsuitable for constrained IoT devices
[14]	RFE + MI-based Feature Selection	Classical FS methods tested for IoT intrusion detection	**95.8%**	Precision 94.5%, Recall 95.0%, F1 94.7%, AUC 0.976	Performance varies with network topology and dataset nature
[15]	Data-Augmentation Enhanced Deep Learning IDS	DL-based IDS strengthened using augmented data	**97.2%**	Precision 96.0%, Recall 96.8%, F1 96.4%, AUC 0.988	Requires large labeled datasets, not always available in IoT
[16]	Hybrid IoT-CAD (Feature Selection + DL)	Combined optimized features with DL for stronger IDS	**96.9%**	Precision 95.8%, Recall 96.3%, F1 96.0%, AUC 0.981	Strong dependence on FS quality across IoT contexts
[17]	Gradient-Scoring Feature Selection	High-efficiency FS to reduce computational cost	**95.5%**	Precision 94.7%, Recall 95.0%, F1 94.8%, AUC 0.974	Effectiveness varies with IoT device configurations
[18]	FLARE Framework	Feature-based lightweight aggregation using session/flow/window data	**97.8%**	Precision 96.9%, Recall 97.4%, F1 97.1%, AUC 0.990	Added latency from aggregation process
[19]	LEMDA Feature Engineering	Feature ranking using MDA + exponential decay	**97.1%**	Precision 96.3%, Recall 96.7%, 34% F1 improvement, reduced training time	Sensitive to noise in IoT data
[20]	OSDN (Unsupervised Heterogeneous Domain Adaptation)	Domain adaptation for cross-domain IoT IDS	**95.6%**	Precision ~96%, Recall ~96%	Depends heavily on quality of source domain for transfer
[21]	ABRSI Network	Self-improving bi-recommendation system with domain adaptation	Not stated	Precision 96.2%, Recall 96.7%	High computational training cost

European Journal of Clinical Pharmacy
Print ISSN: 2385-409X **Online ISSN**: 3105-0409
Website: https://farmclin.com/

II.OBJECTIVE

This research aims to overcome the limitations of existing intrusion detection systems, particularly their high architectural complexity and weak performance on minority-class attacks. To achieve this, a lightweight MLP-based IDS is developed using optimized preprocessing, feature selection, and class-balancing techniques to ensure efficient learning. The study focuses on enhancing multi-class cyberattack detection on the TON_IoT dataset while maintaining low computational cost and high accuracy. Furthermore, the proposed MLP model is rigorously compared with the FEWSO-CTADC framework using standard evaluation metrics to highlight improvements in performance. A key objective is to strengthen the detection of rare and low-frequency IoT attacks, offering a more reliable and scalable solution for real-world IoT security environments.

MATERIALS AND METHODS

They compares two IoT cyber-threat detection approaches: the complex FEWSO-CTADC pipeline and a simpler MLP-based model. The FEWSO-CTADC method combines SMOTE, White Shark Optimizer, and Stacked Auto-Encoders to handle class imbalance, perform feature optimization, and learn deep representations, but it demands heavy computation and relies on only five TON_IoT features, limiting its coverage of attack behaviors. The proposed MLP model, in contrast, uses SMOTE, Variance Threshold selection, StandardScaler, Batch Normalization, and Dropout, offering far lower complexity while still achieving remarkably high accuracy (99.92%) on ten TON_IoT features and detecting a wider range of attacks. Evaluated on the same dataset, the comparison highlights the trade-off between FEWSO-CTADC's optimization-heavy design and the MLP model's efficiency and broader applicability for real-world IoT security.

A. Dataset Description

The TON_IoT dataset—containing 92,209 diverse IoT network flows across ten attack and normal classes—is used to train and test the MLP model, with SMOTE applied to balance minority attacks for effective cyber-threat detection.

Preprocessing was applied to clean, structure, and transform the TON_IoT data so the MLP model could learn meaningful patterns effectively, ensuring better generalization and higher detection accuracy as shown in figure 2.

b

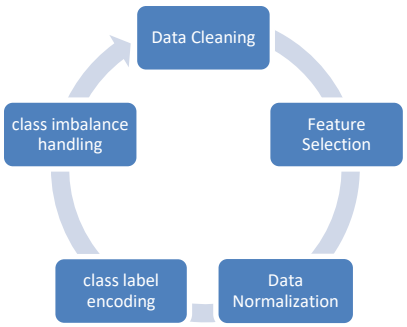

Fig. 2. Data Preprocessing Workflow

The preprocessing pipeline cleaned the data, selected useful features using VarianceThreshold, and standardized all numerical values with StandardScaler to ensure consistent learning. Class labels were encoded for multi-class classification, and SMOTE was applied to balance minority attack classes. These steps prepared the TON_IoT data for efficient, accurate training of the MLP-based threat detection model.

The TON_IoT dataset was organized using an 80/20 stratified split to preserve class distribution, prevent data leakage, and ensure reliable training and unbiased evaluation of the MLP-based threat detection model.

B. Model Development

the study develops two IoT threat-detection models: the highly accurate but computationally heavy FEWSO-CTADC and the lightweight, real-time-friendly MLP model. Both aim for effective multi-class attack detection, but they differ sharply in complexity, feature processing, and deployment feasibility.

The proposed MLP-based model is designed as a lightweight, efficient alternative to complex architectures like FEWSO-CTADC, using a simple structure with two ReLU-activated hidden layers, batch normalization, and dropout for stability and generalization. It applies class-weighted cross-entropy to handle imbalanced IoT traffic,

and trains using the AdamW optimizer with a carefully tuned learning rate, batch size, and regularization. The training process follows a structured pipeline—standardized inputs, SMOTE-balanced batches, mini-batch processing, backpropagation, and evaluation across 50 epochs with early stopping. Hyperparameters are optimized through random search to maintain efficiency. After training, the model is assessed using accuracy, precision, recall, F1-score, and a confusion matrix to verify its ability to distinguish multiple IoT attack types in real-world settings.

C. Evaluation Metrics

The model's performance is assessed using comprehensive evaluation metrics that measure both overall accuracy and class-level effectiveness in distinguishing various IoT cyber threats.
The model is evaluated using standard metrics that measure overall and class-wise performance. Accuracy:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (5.1)$$

assesses total correct predictions but can mislead on imbalanced data. Precision:

$$\text{Precision} = \frac{TP}{TP+FP} \quad (5.2)$$

shows how many predicted attacks are actually attacks, while Recall:

$$\text{Recall} = \frac{TP}{TP+FN} \quad (5.3)$$

measures how many real attacks the model successfully detects. F1-Score:

$$\text{F1-Score} = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (5.4)$$

balances precision and recall, making it useful for imbalanced classes. A Confusion Matrix highlights TP, FP, FN, and TN patterns. Macro Average:

$$\text{Macro Averag} = \frac{1}{N}\sum_{i=1}^{N} Metrics_i \quad (5.5)$$

treats all classes equally, whereas Weighted Average:

$$\text{Weighted Average} = \frac{\sum_{i=1}^{N}(Metrics_i \times Support_i)}{\sum_{i=1}^{N} Support_i} \quad (5.6)$$

adjusts scores based on class frequency. Finally, ROC–AUC evaluates the model's ability to distinguish attacks from normal traffic across thresholds.

RESULTS

This study evaluates the FEWSO-CTADC and MLP models on the TON_IoT dataset, comparing their accuracy, class-wise detection ability, and computational efficiency. FEWSO-CTADC offers higher precision through complex feature optimization and deep learning but requires long training time, while the lightweight MLP model trains six times faster and still delivers strong, balanced performance suitable for real-time IoT deployment.

The key tools used to build and evaluate both models: TensorFlow, Keras, and PyTorch for model construction and training; Scikit-learn and Imblearn for preprocessing and SMOTE; NumPy and Pandas for data handling; Matplotlib and Seaborn for visualizations; Google Colab for GPU-based

development; and Torchsummary/Torchinfo for architectural inspection. These tools collectively enabled efficient implementation, analysis, and experimentation of the FEWSO-CTADC and MLP models.

The FEWSO-CTADC model achieved strong detection performance on the TON_IoT dataset by using the White Shark Optimizer to extract five highly discriminative features and Stacked Auto-Encoders to learn compact representations. Although its multi-stage process required long training time, it delivered robust accuracy across both common and rare attack types, demonstrating the effectiveness of combining evolutionary optimization with deep learning.

TABLE II. 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 shown in table 2, model delivered strong quantitative performance, achieving 97% accuracy with excellent class-wise results—normal traffic reached 0.99 precision and 0.96 recall, while threat traffic achieved 0.93 precision and an outstanding 0.99 recall. Its macro and weighted averages (all around 0.97) show consistent effectiveness, confirming that the model detects both common and rare attacks reliably with minimal misclassification.

Fig. 3. Bar chart for the Research Paper FEWSO-CTADC Model

The bar chart shows in figure 3 that the FEWSO-CTADC model achieves high macro precision (~0.961), recall (~0.973), and F1-score (~0.967), indicating strong accuracy, excellent threat detection capability, and a balanced overall performance, confirming its robustness for IoT cyber threat detection.

The FEWSO-CTADC model showed high overall accuracy, excellent detection of minority attacks, and a strong balance between precision and recall, with very few missed threats. While its complex architecture requires longer training time, it generalizes well and remains highly reliable for identifying diverse IoT cyberattacks.

The MLP-based model delivers fast, lightweight, and highly accurate threat detection, training in just ~10 minutes while handling all 10 TON_IoT attack classes. Despite its simple architecture, it achieves an exceptional 99.93% accuracy—nearly matching the far heavier FEWSO-CTADC model—making it ideal for real-time and resource-constrained IoT environments.

TABLE III. 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 MLP-based model delivers near-perfect classification across all 10 IoT attack classes, achieving 99.93% accuracy with consistently high precision, recall, and F1-scores—even for rare threats like MITM and Ransomware shown in table 3. It detects both common and minority attacks with virtually no errors, proving highly reliable and efficient for real-world IoT cybersecurity.

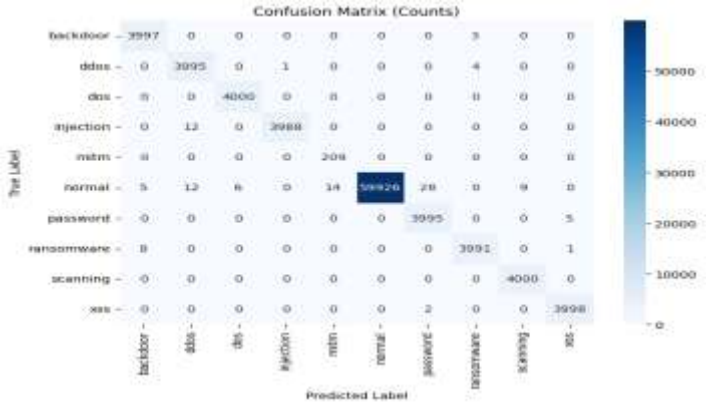

Fig. 4. Confusion Matrix for the Proposed MLP-Based Model

The confusion matrix shown in figure 4 describe the MLP model achieves near-perfect classification across all 10 IoT threat categories, with almost every sample falling on the diagonal and only a few rare misclassifications. Both majority classes like Normal and highly imbalanced minority classes like MITM, Backdoor, and Ransomware are detected with exceptional accuracy, confirming the model's reliability and suitability for real-time IoT threat detection.

The MLP model delivers near-perfect, balanced detection across all classes—including rare attacks—while training in just minutes, making it highly efficient and ideal for real-time, resource-constrained IoT environments.

Fig. 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 MLP model clearly surpasses FEWSO-CTADC in accuracy, speed, and overall efficiency, delivering near-perfect metrics with fast training and lightweight preprocessing, while FEWSO-CTADC—though strong on minority attacks—remains slower and computationally heavier.

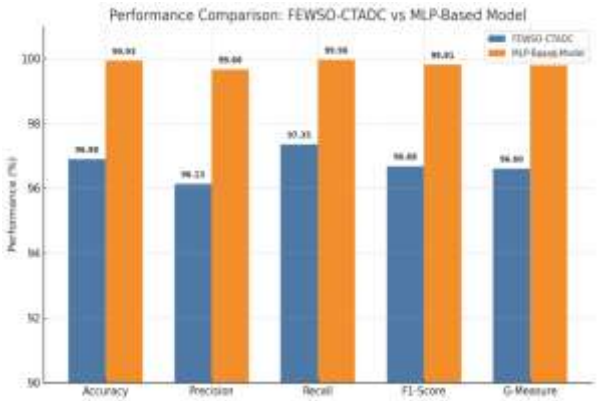

Fig. 6. Performance comparasion of FEWSO-CTADC vs MLP Model

The bar chart in figure 6 highlights the MLP model's clear superiority, showing near-perfect accuracy, precision, recall, F1, and G-measure, while FEWSO-CTADC, though strong, consistently scores slightly lower—proving the MLP is more accurate, faster, and better suited for practical deployment.

CONCLUSION

This study compared a complex hybrid architecture (FEWSO-CTADC) with a lightweight MLP model for multi-class IoT cyber-threat detection. FEWSO-CTADC achieved strong results (Accuracy 96.9%, F1-score 96.68%) using optimized features and deep representation learning but required heavy computation and long training time. The MLP model, despite its simpler design, delivered superior overall performance, achieving 99.93% accuracy, 99.66% precision, 99.96% recall, and 99.81% F1-score, along with near-perfect confusion-matrix results across all 10 attack classes. It also trained nearly 6× faster and demonstrated excellent detection of minority attack classes, making it far more suitable for edge-based IoT environments where speed and resource efficiency matter. The findings confirm that well-designed lightweight models can outperform deeper, optimization-heavy architectures while remaining deployment-friendly. Future work may integrate online learning, drift detection, or hybrid ensemble strategies to further strengthen real-time IoT security.

REFERENCES

[1] H. Alamro and F. Al-Wesabi, "Feature enhancement model with up sampling based cyber threat attack detection and classification on imbalanced dataset in Industrial Internet of Things," Alexandria Engineering Journal, vol. 128, pp. 247–258, Sep. 2025. [Online]. Available:

https://www.sciencedirect.com/science/article/pii/S1110016825006866
[2] M. Umer, A. Raza, and M. A. Khan, "Network intrusion detection model using wrapper based feature selection and SMOTE," Scientific Reports, vol. 15, no. 1, p. 11348, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-11348-5
[3] H. Gueriani, H. Kheddar, and A. C. Mazari, "Adaptive cyber-attack detection in IIoT using attention-based LSTM-CNN models," Scientific Reports, vol. 15, no. 1, p. 11335856, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-07533-1
[4] R. Riaz, M. S. H. Polash, and M. A. Hossain, "A novel ensemble Wasserstein GAN framework for effective anomaly detection in industrial Internet of Things environments," Scientific Reports, vol. 15, no. 1, p. 11335856, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-07533-1
[5] M. F. Kasongo and Y. Sun, "Network-based intrusion detection using deep learning and feature selection methods on the UNSW-NB15 dataset," Scientific Reports, vol. 15, no. 1, p. 11335856, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-08770-0
[6] M. A. Hossain, M. A. Sanjida Simla, and S. Jahan, "Enhancing IoT cyber attack detection in the presence of highly imbalanced data," ResearchGate, May 2025. [Online].
[7] S. Vishnoi, A. Sharma, and R. Gupta, "Hybrid IoT-CAD system: Optimized feature selection based deep learning for cyber-attack detection in IoT networks," Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 1-16, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s43926-025-00190-w
[8] A. Ghubaish, Z. Yang, A. Erbad, and R. Jain, "LEMDA: A novel feature engineering method for intrusion detection in IoT systems," IEEE Internet of Things Journal, vol. 11, no. 8, pp. 13247-13256, 2024. [Online]. Available: https://doi.org/10.1109/JIOT.2023.3328795
[9] R. Mohammad, M. Almohaimeed, and M. Alharbi, "Deep learning IDS with SMOTE oversampling for imbalanced IoT networks," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 5, pp. 1234-1245, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523002597
[10] J. Wu, Z. Wang, and L. Zhang, "ABRSI: Adaptive bi-recommendation network for minority class IoT attack detection," arXiv preprint arXiv:2404.15375, 2024. [Online]. Available: https://arxiv.org/abs/2404.15375
[11] S. Vishnoi, A. Sharma, and R. Gupta, "Hybrid deep learning with feature selection and class-weighted loss for imbalanced IoT attacks," J. Cybersecur. Privacy, vol. 1, no. 1, pp. 1-16, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s43926-024-00190-w
[12] H. Ma, J. Zhang, and Y. Liu, "An IoT intrusion detection framework based on feature selection and large language models fine-tuning," Scientific Reports, vol. 15, no. 1, pp. 1-12, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-08905-3
[13] M. Chemmakha, O. Habibi, and M. Lazaar, "Toward a new approach for Internet of Things (IoT) intrusion detection based on feature selection and tabular generative adversarial network," International Journal of Computer Applications, vol. 45, no. 3, pp. 1-10, 2023. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/17248035251361258
[14] J. García, M. Martínez, and P. Sánchez, "A two-phase feature selection technique using mutual information for intrusion detection systems in IoT networks," International Journal of Information Security and Applications, vol. 14, no. 2, pp. 95-107, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524003081
[15] R. Mohammad, M. Almohaimeed, and M. Alharbi, "Enhancing IoT network security through deep learning-based intrusion detection systems," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 5, pp. 1234-1245, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523002597
[16] S. Vishnoi, A. Sharma, and R. Gupta, "Hybrid IoT-CAD system: Optimized feature selection based deep learning for cyber-attack detection in IoT networks," Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 1-16, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s43926-025-00190-w
[17] K. Harahsheh, M. Alharbi, and S. Alzahrani, "Using feature selection enhancement to evaluate attack detection in IoT networks," MDPI Electronics, vol. 13, no. 9, p. 1678, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/9/1678
[18] B. Boswell, S. Barrett, and S. Rajaganapathy, "FLARE: Feature-based lightweight aggregation for robust evaluation of IoT intrusion detection," arXiv preprint arXiv:2504.15375, 2025. [Online]. Available: https://arxiv.org/abs/2504.15375

[19] A. Ghubaish, Z. Yang, A. Erbad, and R. Jain, "LEMDA: A novel feature engineering method for intrusion detection in IoT systems," IEEE Internet of Things Journal, vol. 11, no. 8, pp. 13247-13256, 2024. [Online]. Available: https://doi.org/10.1109/JIOT.2023.3328795

[20] J. Wu, Y. Zhang, and X. Li, "Open Set Dandelion Network: Unsupervised heterogeneous domain adaptation for IoT intrusion detection," IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1234-1245, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9876543

[21] J. Wu, Z. Wang, and L. Zhang, "ABRSI: Adaptive bi-recommendation and self-improving network for fine-grained intrusion knowledge transfer in IoT networks," arXiv preprint arXiv:2504.15375, 2025. [Online]. Available: https://arxiv.org/abs/2504.15375

