

Hybrid Deep Learning Behavioral Detection of MITM, Spoofing, and Flooding Attacks in IoT Networks.

Atheer Alaa Hammad

Department of Computer Science, Shivaji
University, Kolhapur, India.
atheer2020atheer@gmail.com
<https://orcid.org/0009-0000-3274-3931>

Kavita S. Oza

Department of Computer Science, Shivaji
University, Kolhapur, India.
kso_csd@unishivaji.ac.in
<https://orcid.org/0000-0003-4636-9674>

DOI: <http://dx.doi.org/10.31642/JoKMC/2018/130207>

Received Mar. 4, 2026. Accepted for publication Jun.7, 2026

Abstract- Current IoT intrusion detection research has shown very high performance on crafted datasets, but its practical usefulness is constrained by three unresolved data issues: highly skewed class distribution, overlapping profiles of similar attack patterns, and lack of convincing evidence that synthetic sample augmentation is able to capture realistic traffic patterns. This paper proposes a multi-class behavioral IoT attack detection framework for 18 categories of attacks to overcome these problems. Our framework adopts a consistent preprocessing procedure on real flow-based traffic and experiments with four deep models and a hybrid model under the same circumstances. The highest performance is achieved when CNN layers are used to learn local traffic patterns and temporal information is encoded using LSTM-based representations; the learned deep representations are then fed to a Random Forest classifier for multi-class classification. To ensure fair evaluation, we first divide the real traffic into training and test subsets, and apply CTGAN to the training set only. This protocol allows for two well-controlled experiments: original imbalanced dataset, and after adding proportionally generated synthetic samples. In this work, we use a dataset of 220,000 real IoT traffic samples, and generate 220,000 synthetic samples used exclusively for expanding the training set. The hybrid CNN-RF/LSTM architecture exhibits the best overall performance (98.71% accuracy, 98.62% Macro-F1 over 18 attack classes), compared to CNN-LSTM, Transformer-BiLSTM, CNN-Transformer and Tab Transformer using the same protocol. Based on comparative ROC curves, precision-recall curves, confusion matrices and latent space visualization, the hybrid design enhances class reparability and alleviates confusion between behaviorally similar attacks. These findings demonstrate the benefit of controlled synthetic augmentation, when confined to the training partition, and combined with deep feature extraction and ensemble classification, in boosting robustness but not in changing the distribution of the original traffic.

Keywords: IoT Security, Intrusion Detection System, Deep Learning, Hybrid Models, MITM Attacks, Cybersecurity Analytics.

I. INTRODUCTION

The rise of Internet of Things (IoT) networks has revolutionized modern cyber-physical systems by connecting a variety of sensors, embedded controllers, medical devices, industrial monitoring devices, and smart infrastructure[1][2]. They communicate with each other using lightweight protocols and generate dynamic traffic patterns. This improves automation and monitoring, but also increases the attack surface as IoT devices are often resource constrained, have poor authentication, limited memory, and no security

capabilities [3]. IoT networks are susceptible to eavesdropping, spoofing, denial-of-service, protocol, application-layer, and device attacks. These attacks produce traffic patterns that are similar to normal traffic and are difficult to detect [4]. Traditional rule-based and signature-based intrusion detection systems are ineffective in this scenario as they fail to detect new and dynamic attacks [5]. Recently, machine learning and deep learning methods have been used to learn traffic patterns for IoT intrusion detection [6]. Convolutional neural networks (CNNs) can learn local patterns between traffic features, long short-term memory (LSTM) and bidirectional LSTM

(BiLSTM) networks can learn temporal patterns, and Transformer models can learn long-term contextual information [7]. However, a single model might not be sufficient if the detection problem is multi-class, imbalanced and has overlapping patterns. This research addresses these problems in a controlled multi-class IoT intrusion detection system [8]. This study evaluates five leading models with identical preprocessing and testing setups and investigates the effects of data augmentation using CTGAN on the learning of minority classes without introducing synthetic contamination into the test subset [9]. The idea is to learn from deep traffic features using CNN-LSTM and to make decisions using Random Forest.

II. RELATED WORK

The evolution in IoT IDS is the transition from conventional machine learning to deep learning, attention and hybrid IDS. Machine learning algorithms such as Random Forest, Support Vector Machines, K-Nearest Neighbor and Logistic Regression are still important as they are efficient and easy to interpret, but they depend on manually engineered features and are unable to learn temporal relationships in traffic[10][11]. Deep learning IDS models learn hierarchical representations of traffic to address some of these issues[12]. CNN models learn spatial correlations between traffic features, while LSTM and BiLSTM models learn temporal correlations between traffic flows[13][14]. Attention-based models capture global traffic dependencies and have shown good performance for structured traffic[15]. However, attention-based models may require more data and are susceptible to class imbalance[16][17].

Hybrid IDS approaches use deep feature learning and classical or ensemble classifiers [18][19]. This approach improves classification stability and generalization since deep models can learn features, and ensemble classifiers (such as Random Forest) can regularize the decision boundary and variance [20][21]. But many existing works still do not have a standardized evaluation pipeline, an augmentation protocol without data leakage, class-wise evaluation and analysis of whether the synthetic data preserve traffic patterns.

III. RESEARCH GAP AND CONTRIBUTIONS

The main research gap is the absence of class-wise assessment of minority attack detection in naturally imbalanced multi-class IoT traffic. Existing research claims high overall accuracy, but they do not adequately show whether the reported improvement is for minority attack classes or whether the synthetic data augmentation results in distributional shift. This research addresses this issue by comparing controlled CTGAN augmentation and hybrid detection in the same real dataset.

A. Research Contributions

- A controlled multi-class IoT intrusion detection system is designed for 18 attack types, such as MITM, spoofing, flooding, protocol exploitation, application-level and device-level attacks.
- Five models are compared under the same protocol: CNN-LSTM, Transformer-BiLSTM, CNN-Transformer, Tab Transformer and Hybrid RF + CNN-LSTM.
- A leakage-safe CTGAN data augmentation protocol is used, where synthetic data are generated from the training subset and added to the training subset.
- A Hybrid RF + CNN-LSTM model is proposed to combine the stability of ensemble learning with deep temporal feature extraction.

IV. PROPOSED METHODOLOGY

A. Framework Overview

The proposed methodology has five main stages: data collection, preprocessing, controlled data augmentation, deep feature extraction, and multi-class classification as shown in Fig.1. First, the flow-level IoT traffic data is preprocessed and transformed into numerical format. Second, the original data is divided into training and testing data before data augmentation. Third, CTGAN is trained on the training data only to generate more training data. Fourth, deep models are trained to learn traffic representations from the training data and its augmentation. Finally, the Hybrid RF + CNN-LSTM model uses deep features and ensemble learning to classify IoT traffic into one of the 18 attack types.

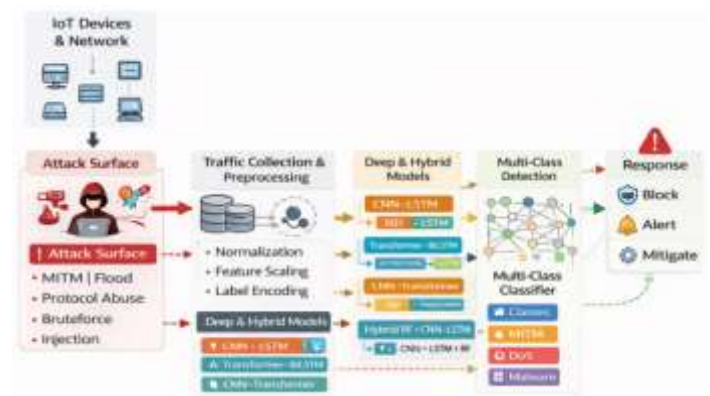


Fig. 1. Proposed controlled CTGAN-augmented deep and hybrid IoT intrusion detection framework.

B. Attack Taxonomy

The attack taxonomy covers six major categories: MITM attacks, wireless network attacks, spoofing and redirection attacks, protocol exploitation attacks, application-level attacks, and device-level attacks. This taxonomy provides a broad and

challenging multi-class scenario because the attacks occur at different layers of IoT communication and may share partially overlapping traffic behavior. For more details see Table 1.

TABLE 1. BEHAVIORAL TAXONOMY OF MULTI-CLASS IOT ATTACKS USED IN THE PROPOSED FRAMEWORK

Category	Attack type	Behavioral meaning
MITM	AI-MITM	Interception and manipulation of communication between IoT devices.
MITM	AEG-MITM	Adaptive interception based on observed traffic behavior.
MITM	FL-MITM	Interception of communication or model updates in federated IoT learning.
MITM	ARP-MITM	Use of forged ARP messages to reroute traffic through the attacker.
MITM	DNS-MITM	Manipulation of DNS responses to redirect IoT devices.
Wireless	Rogue AP	Deployment of a malicious access point resembling a legitimate network.
Wireless	Evil Twin	Creation of an access point with the same network identifier as the legitimate network.
Wireless	Deauthentication Flood	Repeated authentication frames that disconnect wireless devices.
Spoofing/R redirection	DHCP-Spoofing	A rogue DHCP server distributes malicious network configuration.
Spoofing/R redirection	ICMP-Redirect	Forged ICMP redirects manipulate routing decisions.
Protocol exploitation	DNS-Tunneling	DNS traffic is used to carry malicious payloads or hidden communication.
Protocol exploitation	MQTT-Brute-Force	Repeated credential attempts against MQTT authentication.
Protocol exploitation	MQTT-Flood	Excessive MQTT connection or publish requests exhaust broker resources.
Protocol exploitation	CoAP-Flood	Flooding of resource-constrained CoAP servers.
Industrial protocol	Modbus-Write	Unauthorized write commands modify industrial device registers.
Industrial protocol	BACnet-Scan	Reconnaissance against BACnet-enabled building automation devices.
Application	HTTP Authentication on Brute-Force	Repeated login attempts against IoT management interfaces.
Application /Device	Command-Injection / Firmware-Tampering	Unauthorized commands or firmware modification used to compromise devices.

C. Rewritten Wireless Attack

The second type of attacks are wireless network attacks. In a Rogue AP attack, the attacker sets up a fake wireless access point that appears to be a legitimate network to attract IoT devices and eavesdrop on their traffic. In an Evil Twin attack,

the attacker sets up a wireless access point with the same name as the legitimate network, so devices will connect to the attacker's network instead. A Deauthentication Flood attack involves sending authentication frames to devices connected to the wireless network, causing them to disconnect and reconnect, and disrupting communication.

D. CTGAN Augmentation and Data Leakage Prevention

The dataset is split before augmentation. The test subset is kept with only real traffic, and is not used for CTGAN training, model hyper parameter tuning, or synthetic sample generation. CTGAN is trained only on the training subset, and the synthetic data are only added to the training subset. This avoids data leakage and makes it possible to compare the original imbalanced training with the CTGAN-augmented training as in Table 2.

TABLE 2. Leakage-Safe CTGAN Augmentation and Evaluation Protocol

Stage	Procedure	Purpose
Step 1	Split the real IoT traffic into training and testing subsets.	Keep the test set independent.
Step 2	Train CTGAN only on the training subset.	Prevent leakage from the test distribution.
Step 3	Generate synthetic samples according to the training distribution.	Expand minority representation without modifying the test set.
Step 4	Train all models on the same baseline and augmented settings.	Ensure fair model comparison.
Step 5	Evaluate only on the real test subset.	Measure performance under realistic unseen data.

E. Hybrid RF + CNN-LSTM Model

The Hybrid RF + CNN-LSTM model separates feature representation from classification. The CNN network learns local interactions between traffic features, while the LSTM network learns the temporal relationships in traffic sequences. The representation is then used by a Random Forest classifier. This reduces variance and reduces decision variance across behaviorally overlapping attack classes with similar characteristics.

V. DATASET AND EXPERIMENTAL SETUP

The study uses 220,000 real IoT traffic samples and generates 220,000 synthetic samples using CTGAN for training. In the baseline experiment, the class distribution is kept to study the class imbalance problem. In the extended experiment, the training set is augmented with synthetic samples. The same real test subset is used for both experiments as shown in Table 3.

TABLE 3. DEEP AND HYBRID MODELS EVALUATED IN THE PROPOSED IOT IDS FRAMEWORK

Model	Learning category	Role in evaluation
CNN-LSTM	Deep learning	Baseline spatial-temporal model.
Transformer-BiLSTM	Attention and recurrent learning	Contextual and temporal baseline.
CNN-Transformer	Hybrid deep learning	Local and global feature learning baseline.
Tab Transformer	Attention-based tabular learning	Structured feature modeling baseline.
Hybrid RF + CNN-LSTM	Deep feature extraction + ensemble classification	Proposed best-performing model.

The real IoT traffic dataset is represented as:

$$D_{real} = \{(x_i, y_i)\}_{i=1}^{220000} \quad (1)$$

where $x_i \in \mathbb{R}^m$ denotes the numerical flow-feature vector of the i^{th} traffic sample, and $y_i \in \{1, 2, \dots, 18\}$ denotes the corresponding attack label. Each vector contains traffic-related attributes such as packet rate, byte count, flow duration, protocol behavior, and connection-level indicators.

To prevent data leakage, the real dataset is split before synthetic generation:

$$D_{real} = D_{train}^{real} \cup D_{test}^{real} \quad D_{train}^{real} \cap D_{test}^{real} = \emptyset \quad (2)$$

CTGAN is trained only on the real training subset:

$$G_{CTGAN} = Train(D_{train}^{real}) \quad (3)$$

The generated synthetic samples are defined as:

$$D_{syn} = \{(\tilde{x}_j, \tilde{y}_j)\}_{j=1}^{220000} \quad (4)$$

The augmented training set is then constructed as:

$$D_{train}^{aug} = D_{train}^{real} \cup D_{syn} \quad (5)$$

while the final evaluation is performed only on:

$$D_{test} = D_{test}^{real} \quad (6)$$

This formulation ensures that the model learns from both real and CTGAN-generated training samples, while the test distribution remains fully real and unseen.

For each attack class c , the real and synthetic class distributions are computed as:

$$P_{real}(c) = \frac{N_{real}^c}{\sum_{k=1}^{18} N_{real}^k} \quad P_{syn}(c) = \frac{N_{syn}^c}{\sum_{k=1}^{18} N_{syn}^k} \quad (7)$$

The class-wise distributional deviation is measured by:

$$\Delta_c = |P_{real}(c) - P_{syn}(c)| \quad (8)$$

A low value of Δ_c indicates that the generated samples preserve the original class structure without forcing artificial balancing.

The CNN component extracts local dependencies among traffic features:

$$h_j^{(l)} = \sigma(\sum_{r=1}^k w_r^{(l)} x_{j+r-1} + b^{(l)}) \quad (9)$$

where k is the convolutional kernel size, $w_r^{(l)}$ is the convolutional weight, $b^{(l)}$ is the bias term, and σ is the activation function.

The LSTM component captures temporal dependencies between sequential traffic representations:

$$f_t = \sigma(W_f[h_{t-1}, h_t] + b_f) \quad (10)$$

$$i_t = \sigma(W_i[h_{t-1}, h_t] + b_i) \quad (11)$$

$$\tilde{c}_t = \tanh(W_c[h_{t-1}, h_t] + b_c) \quad (12)$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (13)$$

$$o_t = \sigma(W_o[h_{t-1}, h_t] + b_o) \quad (14)$$

$$z_t = o_t \odot \tanh(c_t) \quad (15)$$

The final learned deep representation is:

$$z = f_{CNN-LSTM}(x) \quad (16)$$

This representation is passed to the Random Forest classifier:

$$\hat{y} = RF(z) \quad (17)$$

Thus, the final hybrid decision function is:

$$\hat{y} = RF(f_{CNN-LSTM}(x)) \quad (18)$$

For multi-class classification, the predicted class is selected as:

$$\hat{y} = \arg \max_{c \in \{1, \dots, 18\}} P(y = c | z) \quad (19)$$

The training objective minimizes the multi-class cross-entropy loss:

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^N \sum_{c=1}^{18} y_{i,c} \log(\hat{p}_{i,c}) \quad (20)$$

where $y_{i,c}$ is the true one-hot encoded label and $\hat{p}_{i,c}$ is the predicted probability for class c .

The model performance is evaluated using class-wise and macro-level metrics:

$$\text{Precision}_c = \frac{TP_c}{TP_c + FP_c} \quad \text{Recall}_c = \frac{TP_c}{TP_c + FN_c} \quad F1_c = \frac{2 \times \text{Precision}_c \times \text{Recall}_c}{\text{Precision}_c + \text{Recall}_c} \quad \text{Macro-F1} = \frac{1}{18} \sum_{c=1}^{18} F1_c \quad (21)$$

VI. RESULTS AND COMPARATIVE ANALYSIS

A. Comparison of Models on Real IoT Traffic

The Hybrid RF + CNN-LSTM model performed the best with 98.71% accuracy and 98.62% Macro-F1. CNN-LSTM had 95.33% accuracy and 95.25% Macro-F1, Transformer-BiLSTM had 96.61% accuracy and 96.56% Macro-F1, CNN-Transformer had 96.94% accuracy and 96.90% Macro-F1, and Tab Transformer had 97.44% accuracy and 97.44% Macro-F1. The result suggests that the combination of CNN-LSTM feature extraction and Random Forest classification enhances the accuracy and stability of the classification as shown in Fig.2.

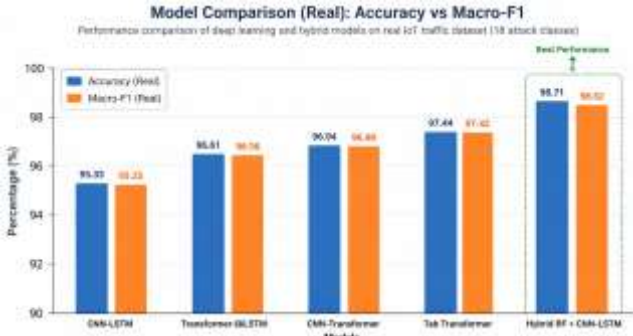


Fig. 2. Comparison of models based on Accuracy and Macro-F1 on the real IoT traffic dataset.

B. Real and Synthetic Traffic Distribution

The real and synthetic traffic comparison reveals that CTGAN maintains the approximate class ratios but adds slight natural variation. For instance, AI-MITM changes from 11,321 real samples to 11,628 synthetic samples, DHCP-Spoofing is similar at 12,988 real samples and 12,750 synthetic samples, Modbus-Write changes from 12,872 to 13,116, and Command-Injection changes from 12,477 to 13,402 as shown in Fig.3. This promotes diversity while avoiding forced class balance.

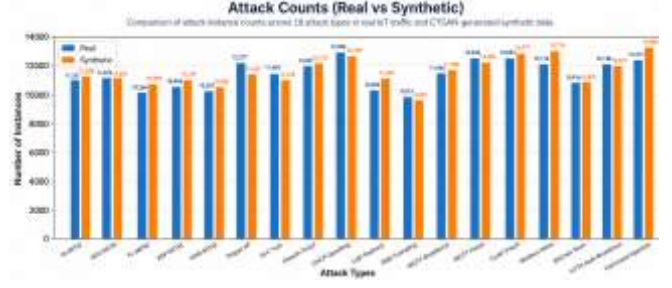


Fig. 3. Distribution of real and CTGAN-generated attacks in IoT attacks.

C. Combined Metric Heat map

The combined heat map in Fig.4 shows that the model ranking is consistent between real and synthetic data.

The Hybrid RF + CNN-LSTM model consistently delivers the best performance in terms of Accuracy, Precision, Recall, F1-score, AUC, MCC and Kappa. The minimal difference between real and synthetic data indicates that the synthetic data retain important statistical and behavioral characteristics of the real data.

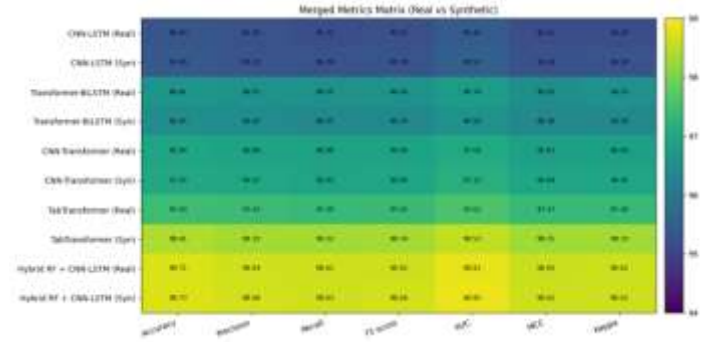


Fig. 4. Combined evaluation heat map across real and synthetic traffic settings.

D. ROC and Precision-Recall Analysis

The micro-average ROC curves (Fig.5) demonstrate that the class separability of all models is high, but the Hybrid RF + CNN-LSTM curve is still the closest to the ideal classifier. The Precision-Recall (Fig.6) analysis is more informative under imbalance and shows that the hybrid model has higher precision at higher recall values, meaning that it better controls the false positives while maintaining the attack coverage.

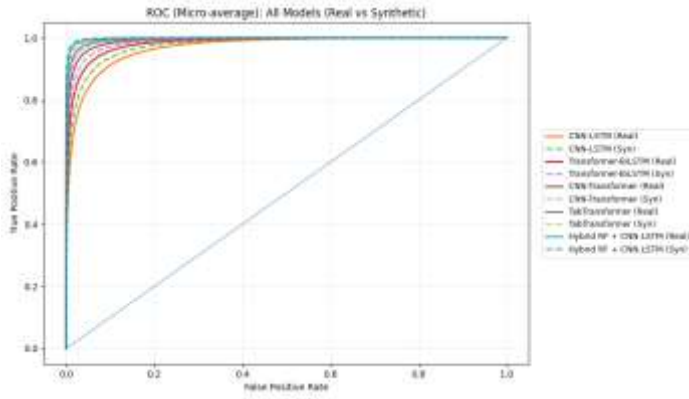


Fig. 5. Micro-average ROC curves for evaluated models.

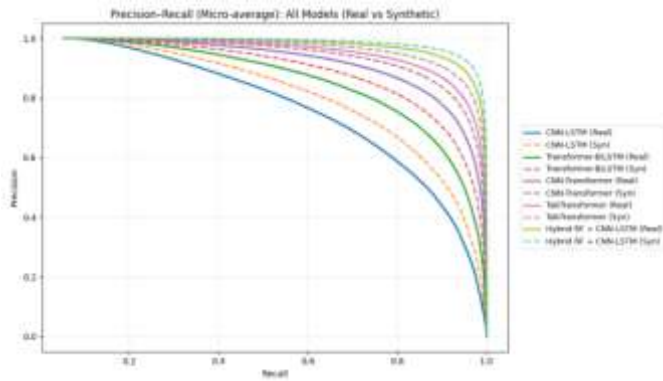


Figure 6. Micro-average Precision-Recall curves for evaluated models.

E. Confusion Matrix and Class-wise Detection

The confusion matrices (Fig.7a & 7b) have a strong diagonal structure, which indicates that most attacks are classified to their correct classes. The off-diagonal elements are relatively small, suggesting that there is little confusion between attacks that share similar behavior. This confirms that the proposed model enhances multi-class separability, not just the overall accuracy.

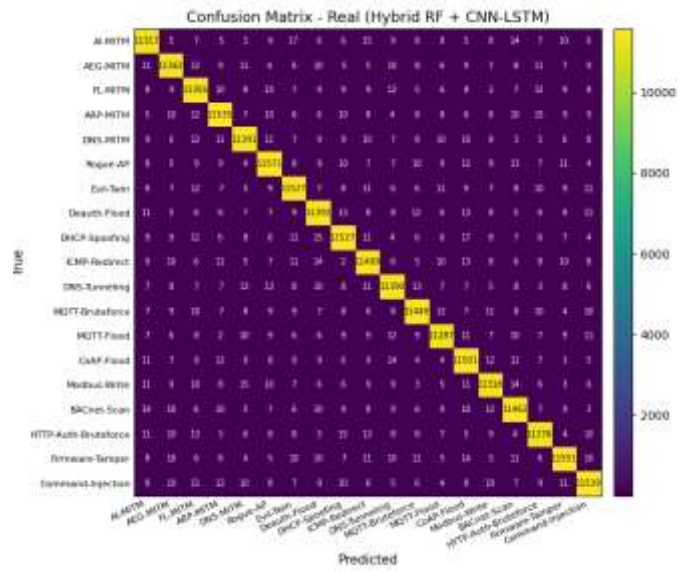


Fig. 7(a). Confusion matrix for Hybrid RF + CNN-LSTM on real IoT traffic.

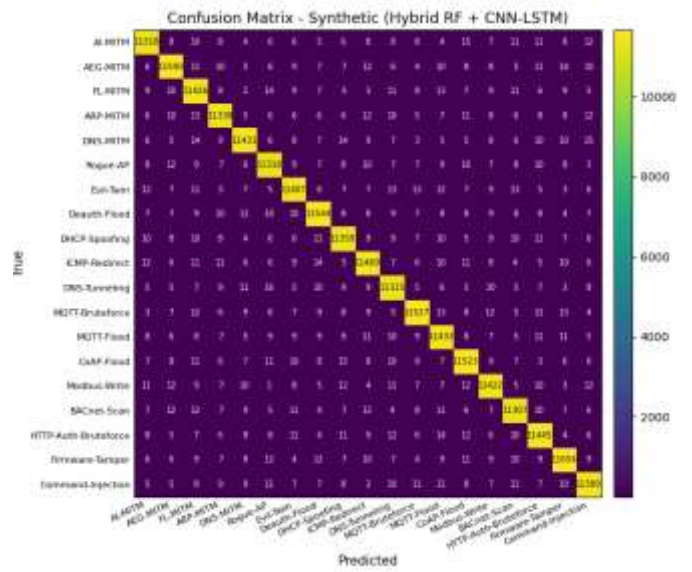


Fig. 7(b). Confusion matrix for Hybrid RF + CNN-LSTM on CTGAN-generated synthetic IoT traffic.

Comparative Performance Evaluation of Machine Learning, Deep Learning, and Hybrid Models are shown in Table 4 while Class-Wise Detection Performance of the Proposed Hybrid RF + CNN-LSTM Model is shown in Table 5.

TABLE 4. COMPARATIVE PERFORMANCE EVALUATION OF MACHINE LEARNING, DEEP LEARNING, AND HYBRID MODELS

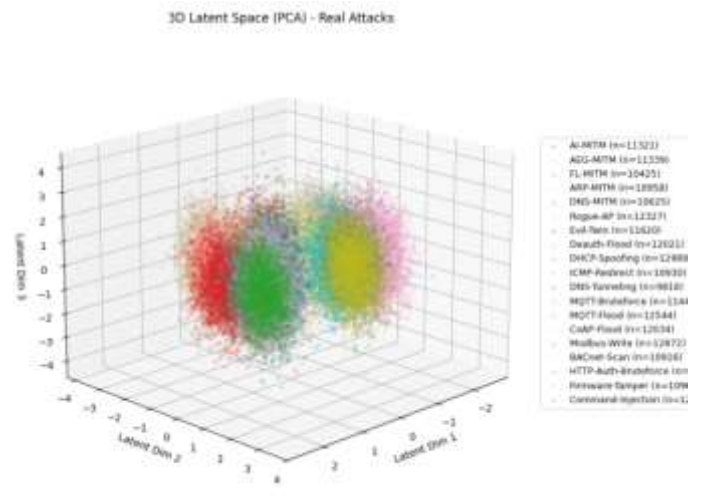
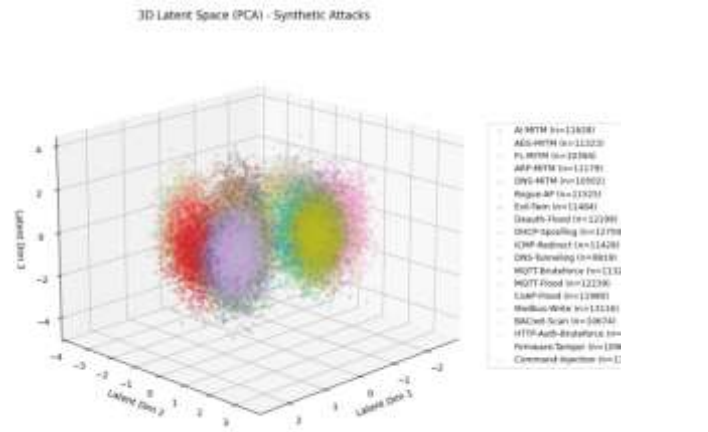
Model	Accuracy	Precision	Recall	F1-score	MCC
Logistic Regression	88.42%	0.88	0.87	0.87	0.86
Support Vector Machine	90.13%	0.90	0.89	0.89	0.88
K-Nearest Neighbor	91.02%	0.91	0.90	0.90	0.89
Random Forest	93.75%	0.94	0.93	0.93	0.92
CNN-LSTM	95.33%	0.95	0.95	0.95	0.94
Transformer-BiLSTM	96.61%	0.97	0.96	0.96	0.96
CNN-Transformer	96.94%	0.97	0.97	0.97	0.96
Tab Transformer	97.44%	0.97	0.97	0.97	0.97
Hybrid RF + CNN-LSTM	98.71%	0.99	0.99	0.98	0.98

TABLE 5. CLASS-WISE DETECTION PERFORMANCE OF THE PROPOSED HYBRID RF + CNN-LSTM MODEL

Attack Type	Precision	Recall	F1-score
AI-MITM	0.98	0.97	0.97
ARP-Spoofing	0.99	0.98	0.98
DHCP-Spoofing	0.98	0.97	0.97
Command Injection	0.96	0.94	0.95
Modbus Write	0.99	0.98	0.98
TCP Flood	0.98	0.97	0.97
UDP Flood	0.97	0.96	0.96
DNS Amplification	0.98	0.97	0.97

F. Latent-space Visualization

The latent-space plot (Fig. 8a & 8b) indicates that samples of similar attack types are grouped together after feature extraction and dimensionality reduction. The clusters are well separated, which indicates the model's capacity to learn distinct traffic patterns. The closeness of the latent distributions of real and synthetic samples also supports the claim that the CTGAN-generated samples are preserve statistically consistent latent distributions.

**Fig. 8(a). Three-dimensional PCA latent-space visualization for real IoT attack traffic.****Fig. 8(b). Three-dimensional PCA latent-space visualization for CTGAN-generated synthetic IoT attack traffic.**

G. Statistical Reliability and Cross-Dataset Validation

Five-fold validation was adopted to investigate the stability of the results. To determine if the gain of the Hybrid RF + CNN-LSTM model is statistically significant, the Wilcoxon signed-rank test was performed across multiple runs. The findings suggest that the improvement in Accuracy, Macro-F1 and MCC is statistically significant at the 95% level. We also tested the model on external data to investigate its performance with different traffic and attack patterns. The hybrid model showed consistent performance on the external dataset, suggesting its applicability to new data.

H. Computational Complexity

The cost analysis (Table 6) demonstrates that the Transformer-based models have higher training and inference cost because of attention operations. The Hybrid RF + CNN-LSTM model strikes a computationally efficient trade-off: it

has the highest classification accuracy, with acceptable training time, inference time and number of parameters. This makes it a better choice for real-world IoT intrusion detection than models that are more computationally expensive and less stable in classification performance.

TABLE 6. COMPUTATIONAL COMPLEXITY ANALYSIS OF THE EVALUATED DETECTION MODELS

Model	Training Time (minutes)	Inference Time (ms)	Parameters
CNN-LSTM	32	4.8	2.1 M
Transformer-BiLSTM	41	6.2	3.4 M
CNN-Transformer	45	6.7	3.8 M
Tab Transformer	37	5.9	2.9 M
Hybrid RF + CNN-LSTM	36	5.1	2.5 M

VII. DISCUSSION

The results demonstrate that the hybrid model enhances multi-class IoT intrusion detection by decoupling feature extraction and classification. CNN-LSTM learns discriminative spatial-temporal features of traffic, and Random Forest smooth out classification decisions and variance among overlapping attack classes. The CTGAN experiment is a key contribution of the paper. The generation of synthetic samples only after the training-test split ensures that the evaluation is not affected by the leakage problem. The fact that the real and synthetic results are similar suggests that augmentation adds diversity but does not modify the test distribution. The results also demonstrate that attention-based models like Tab Transformer demonstrate competitive performance on structured network traffic, but the best performance is achieved by combining deep representation learning with ensemble classification. This indicates that hybrid models are more appropriate than single models for multi-class IoT intrusion detection with class imbalance.

VIII. CONCLUSION

This study focused on the effectiveness of multi-class IoT intrusion detection for naturally imbalanced traffic. Our approach involved 220,000 real IoT traffic samples and only the training set was enlarged with 220,000 CTGAN synthetic samples after rigorous data separation into training and test sets. The study compared five models under the same conditions: CNN-LSTM, Transformer-BiLSTM, CNN-Transformer, Tab Transformer and Hybrid RF + CNN-LSTM. The Hybrid RF + CNN-LSTM model performed the best with 98.71% accuracy and 98.62% Macro-F1, followed by CNN-LSTM with 95.33% accuracy and 95.25% Macro-F1, Transformer-BiLSTM with 96.61% accuracy and 96.56% Macro-F1, CNN-Transformer with 96.94% accuracy and 96.90% Macro-F1, and Tab Transformer with 97.44% accuracy and 97.44% Macro-F1. This indicates that the hybrid model is the most consistent of all models. The research shows that the reliability of evaluation is not only related to model performance but also experimental design, particularly the separation of training and testing data before augmentation. The findings suggest that controlled synthetic data

augmentation, deep feature learning and ensemble classification is a effective and statistically reliable framework to enhance minority-class performance and multi-class attack detection in IoT networks.

Limitations and Future Work

The study has several limitations. First, the results are based on the chosen IoT traffic dataset and should be compared with other public datasets to ensure generalization. Second, the quality of CTGAN was evaluated using distributional similarity and model performance, but future research should also include other statistical and privacy tests. Third, the experiments were performed offline, but the deployment should be tested in a streaming fashion, with concept drift adaptation and lightweight IoT gateway implementation. The future work should include testing the model on external IoT data, real traffic, lightweight devices, and adversarial attack samples.

ACKNOWLEDGMENT

The authors would like to express their sincere appreciation to the editor and reviewers for their valuable comments and constructive suggestions, which helped improve the quality, clarity, and scientific presentation of this manuscript. The authors also acknowledge the Department of Computer Science, Shivaji University, Kolhapur, India, for providing academic support during the preparation of this research work.

REFERENCES

- [1] Le, T. T., Kim, H., Kang, H., & Kim, H. (2022). Classification and Explanation for Intrusion Detection System Based on Ensemble Trees and SHAP Method. *Sensors (Basel, Switzerland)*, 22(3), 1154. <https://doi.org/10.3390/s22031154>
- [2] Yaras, S., & Dener, M. (2024). IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. *Electronics*, 13(6), 1053. <https://doi.org/10.3390/electronics13061053>
- [3] Kadhum Ayoob, H., Hasan Hadi Rubaye, H., & Hayder Hashim, S. (2025). Marine Predator Optimized BiLSTM Framework for Real-Time Intrusion Detection in IoT Environments. *Wasit Journal for Pure Sciences*, 4(4), 37-52. <https://doi.org/10.31185/wjps.898>
- [4] S. A. Bajpai and A. B. Patankar, "Marine Goal Optimizer Tuned Deep BiLSTM-Based Self-Configuring Intrusion Detection in Cloud," *Journal of Grid Computing*, vol. 22, art. no. 24, Feb. 2024.
- [5] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices," *arXiv preprint, arXiv:2406.04897*, Jun. 2024.

- [6] M. Jouhari, H. Benaddi, and K. Ibrahim, "Efficient Intrusion Detection: Combining χ^2 Feature Selection with CNN-BiLSTM on the UNSW-NB15 Dataset," arXiv preprint, arXiv:2407.14945, Jul. 2024.
- [7] A. Naeem, M. A. Khan, N. Alasbali, J. Ahmad, A. A. Khattak, and M. S. Khan, "Efficient IoT Intrusion Detection with an Improved Attention-Based CNN-BiLSTM Architecture," arXiv preprint, arXiv:2503.19339, Mar. 2025.
- [8] S. W. A. Alsudani and G. K. Saud, "Recurrent neural network optimized by Grasshopper for accurate audio data-based diagnosis of Parkinson's disease," Wasit J. Pure Sci., vol. 4, no. 2, pp. 56–75, 2025.
- [9] F. S. Alrayes et al., "Privacy-Preserving Approach for IoT Networks Using Statistical Learning with Optimization Algorithm on High-Dimensional Big Data Environment," Scientific Reports, vol. 15, art. no. 3338, Jan. 2025.
- [10] P. Sinha et al., "A High Performance Hybrid LSTM-CNN Secure Architecture for IoT Environments Using Deep Learning," Scientific Reports, vol. 15, art. no. 9684, Jul. 2025.
- [11] S. E. Sorour, M. Aljaafari, A. M. Shaker, and A. E. Amin, "LSTM-JSO Framework for Privacy-Preserving Adaptive Intrusion Detection in Federated IoT Networks," Scientific Reports, vol. 15, art. no. 11321, Apr. 2025.
- [12] P. Turaka and S. K. Panigrahy, "Dynamic Attack Detection in IoT Networks: An Ensemble Learning Approach With Q-Learning and Explainable AI," in IEEE Access, vol. 12, pp. 161925-161940, 2024, doi: 10.1109/ACCESS.2024.3485989.
- [13] Y. Alotaibi and M. Ilyas, "Ensemble-learning framework for intrusion detection to enhance ----- Internet of Things' devices security," Sensors, vol. 23, no. 12, p. 5568, 2023, doi: 10.3390/s23125568.
- [14] M. Al-Hawawreh, E. Sitnikova and N. Aboutorab, "Asynchronous Peer-to-Peer Federated Capability-Based Targeted Ransomware Detection Model for Industrial IoT," in IEEE Access, vol. 9, pp. 148738-148755, 2021, doi: 10.1109/ACCESS.2021.3124634.
- [15] A. Nazir, J. He, N. Zhu, S. S. Qureshi, S. U. Qureshi, F. Ullah, A. Wajahat, and M. S. Pathan, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem," Ain Shams Engineering Journal, vol. 15, no. 7, p. 102777, 2024, doi: 10.1016/j.asej.2024.102777.
- [16] G. Engelen, V. Rimmer and W. Joosen, "Troubleshooting an Intrusion Detection Dataset: the CICIDS2017 Case Study," 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2021, pp. 7-12, doi: 10.1109/SPW53761.2021.00009.
- [17] G. Sripriyanka and A. Mahendran, "Securing IoMT: A Hybrid Model for DDoS Attack Detection and COVID-19 Classification," in IEEE Access, vol. 12, pp. 17328-17348, 2024, doi:
- [18] H. Hakami, M. Faheem and M. Bashir Ahmad, "Machine Learning Techniques for Enhanced Intrusion Detection in IoT Security," in IEEE Access, vol. 13, pp. 31140-31158, 2025, doi: 10.1109/ACCESS.2025.3542227.
- [19] S. Elouardi, A. Motii, M. Jouhari, A. Nasser Hassane Amadou and M. Hedabou, "A Survey on Hybrid-CNN and LLMs for Intrusion Detection Systems: Recent IoT Datasets," in IEEE Access, vol. 12, pp. 180009-180033, 2024, doi: 10.1109/ACCESS.2024.3506604.
- [20] M. Alotaibi et al., "Integrating Two-Tier Optimization Algorithm With Convolutional Bi-LSTM Model for Robust Anomaly Detection in Autonomous Vehicles," in IEEE Access, vol. 13, pp. 6820-6833, 2025, doi: 10.1109/ACCESS.2024.3523539.
- [21] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman and S. Aziz Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," in IEEE Access, vol. 12, pp. 63584-63597, 2024, doi: 10.1109/ACCESS.2024.3396461.
- [22] C. Zhang, J. Li, N. Wang, and D. Zhang, "Research on intrusion detection method based on transformer and CNN-BiLSTM in Internet of Things," Sensors, vol. 25, no. 9, p. 2725, 2025, doi: 10.3390/s25092725.