
Deep Pattern Classification Model for Detecting Malicious Network Traffic in IoT-Based Smart Home Environments

Dr. S.Selvakumar and Dr. S. Periyasamy

Guest Faculty, Centre for Distance and Online Education, Periyar University, Salem

Guest Faculty, Department of Computer science, Government Arts and Science College, Harur, Dharmapuri

info_selva@periyaruniversity.ac.in

ABSTRACT

The rapid deployment of Internet of Things (IoT) devices in smart home environments increases exposure to malicious network traffic, making accurate and efficient traffic classification essential for protecting connected devices and services. Existing intrusion detection and traffic classification approaches often face challenges in recognizing diverse attack patterns, handling complex traffic characteristics, and maintaining reliable detection performance. To address these limitations, this study proposes a Deep Pattern Classification Model for Detecting Malicious Network Traffic in IoT-Based Smart Home Environments (DPC-MNT-SHE). The proposed model performs network traffic preprocessing, feature representation, deep pattern learning, and multi-class malicious traffic classification using the RT-IoT2022 dataset. DPC-MNT-SHE is built for detecting both normal and malicious traffic patterns and to enhance the discriminative capability over heterogeneous IoT network behaviors. Experimental assessment shows DPC-MNT-SHE achieves 98.5% accuracy, 98.6% precision, 96.5% recall and 98.35% F1-score, which shows its effectiveness in the classification of malicious network traffic over IoT based smart-home environment. The results demonstrate that DPC-MNT-SHE can effectively learn complex traffic patterns and support reliable network security monitoring. Thus, the proposed framework is a practical solution for enhancing malicious traffic detection in IoT-equipped smart homes using deep learning.

Keywords: Internet of Things (IoT); Smart Home Security; Malicious Network Traffic Detection; Deep Learning; Network Traffic Classification; Intrusion Detection.

1. Introduction

The rapid expansion of Internet of Things (IoT) technologies has transformed smart homes by enabling interconnected devices, intelligent automation, remote monitoring, and real-time services. However, the continuous exchange of network traffic among heterogeneous IoT devices increases the attack surface and creates opportunities for botnets, denial-of-service (DoS), distributed denial-of-service (DDoS), malware, and other malicious activities. Thus, identification and classification of malicious network traffic have become a necessity to ensure the security, availability, and reliability of smart home environments based on IoT. Machine learning and deep learning approaches have been studied for this purpose as these methods can automatically learn discriminative features from complex network traffic. Lightweight detection has also been focused on, since many IoT devices are resource and computation limited, which has encouraged the creation of quantized models of machine learning for efficient detection of botnets in IoT networks [1]. Despite these developments, existing IoT intrusion detection approaches continue to encounter several challenges. The IoT traffic is very heterogeneous, dynamically changing, and possesses several distinct modes of communication,

hence, it is hard for malicious traffic to be consistently detected. Conventional machine-learning methods rely heavily on features selected by humans, and have limited ability to capture the complex nonlinear relationship between network traffic. Anomaly detection techniques based on machine learning have been used for DoS attack detection in IoT networks, where the detection accuracy is related to the characteristics of the traffic types and the choice of learning algorithms used [2]. Moreover, smart-home communication poses patterns that are protocol and device specific and demand dedicated analysis. Therefore, the availability of realistic smart-home traffic is an important element for the development and evaluation of reliable detection models. The diversity and complexity of IoT communication patterns are illustrated by a real smart-home environment traffic dataset that is collected from various Zigbee devices and decrypted [3]. Deep learning has provided improved opportunities for automatically learning hierarchical representations from network traffic; however, existing studies often concentrate on individual attack categories, specific protocols, computational efficiency, or particular detection scenarios. The continuous evolution toward optimal use of deep architectures has been explored by investigating an attention-GRU framework optimized by binary particle swarm optimization for improving IoT intrusion detection [4]. Likewise, semi-supervised detection of encrypted malicious traffic based on a multimodal approach to traffic characteristics takes into account the challenges posed by extracting useful information, as traffic content is typically hidden [5]. Federated learning with knowledge distillation has also been investigated for smart-home intrusion detection to enhance distributed security without compromising data privacy [6]. Hybrid deep learning has also been applied to DDoS detection in IoT networks, indicating the potential of combining multiple deep representations for recognizing complex attack behaviors [7]. However, there is a lack of literature regarding the development of a unified deep pattern classification framework just focusing on the identification of various types of malicious network traffic in IoT based smart-home environment. The related studies can be focused at detecting botnets, DoS/DDoS attacks, encrypted traffic, distributed learning, anomaly detection or overall intrusion detection without learning various types of malicious traffics comprehensively. Genetic-algorithm-assisted ensemble anomaly detection has been investigated for securing IoT communications [8], while deep reinforcement learning has been used for IoT malware botnet detection [9]. More recently, adaptive IoT intrusion detection based on graph neural pattern learning has been suggested for large-scale IoT networks, which further proves the need for learning structural and behavior traffic patterns [10]. To overcome these drawbacks, this work introduces DPC-MNT-SHE which is a holistic framework based on a RT-IoT2022 dataset for preprocessing, deep pattern representation, and malicious traffic classification. The aim of the model is to ensure the effective identification of heterogeneous IoT attack behaviors in a smart home environment while ensuring reliable security monitoring.

Contributions of the Paper

- To develop DPC-MNT-SHE for learning discriminative deep traffic patterns and accurately classifying diverse malicious IoT network behaviors effectively.
- To embed hierarchical features graph and deep pattern learning for discriminating between normal and malicious traffic inside smart-home environments.
- To compare the performance of accuracy, precision, recall, and F1-score of DPC-MNT-SHE in RT-IoT2022 to achieve comprehensive malicious traffic classification.

2. Literature Survey

Anitha et al. [11] addressed malicious traffic detection in smart devices by introducing BI-LSTM–CNN Deep Learning (Bi-LSTM–CNN-DL), which captures temporal and spatial traffic features for classification. The real-world deployment and generalization of it may be hindered by the methodology's computational complexity and the characteristics of the dataset. Watanabe et al. [12] addressed evolving malicious traffic detection in IoT smart homes by introducing Self-Adaptive Traffic Anomaly Detection (SATAD), which dynamically updates its machine-learning model using newly captured honeypot traffic. Analysis of pre-captured malware traffic, real-time malware traffic and publicly shared malware traffic showed higher detection rates but continuous data collection and updating of the model comes with operational costs.

Wang et al. [13] discussed the issue of limited generalization in heterogeneous IoT smart-home environments. They introduced the Transformer-Based IoT Intrusion Detection (T-IoT-ID) method, which employs self-attention for contextual traffic representation. Using the ToN_IoT dataset, T-IoT-ID achieved 98.39% binary and 97.06% multiclass accuracy, demonstrating effective intrusion detection. Abdusalomov et al. [14] addressed the need for accurate and scalable intrusion detection in smart-home IoT networks by introducing a Harmony Search Algorithm-enhanced Extra Trees classifier for hyperparameter optimization. The model was tested with a real-time dataset that included 105 IoT devices with three scenarios such as binary, 8-class, and 34-class.

Reis [15] discussed privacy, latency and computational limitations when implementing cybersecurity in a centralized way for the IoT in smart-home scenarios with 5G. To overcome this centralization of raw data sharing, the proposed Edge-FLGuard+ framework adopts lightweight federated learning, edge processing as well as anomaly detection. It was assessed with TON_IoT and CIC-IDS2018 datasets, where the subsets were processed and used in experiments. However, Reis and Serôdio [16] discussed real-time anomaly detection in smart homes, in which the use of cloud processing introduces latency and privacy issues. They proposed the Edge-AI system based on the Isolation Forest and LSTM Autoencoder models for synthetic temperature, motion and energy data. Anomaly-detection was shown but generalization in the real world might be restricted due to synthetic data.

Wahab et al. [17] addressed DDoS intrusion detection in IoT networks by introducing CNN, DNN, and Transformer architectures for binary, three-class, and 12-class classification. Using CIC-IoT2023, preprocessing incorporated normalization and SMOTE. The models achieved 99.2%, 99.0%, and 98.8% binary accuracy, while 12-class accuracy reached 93.0%, 92.7%, and 92.5%. However, one of the drawbacks is the lack of cross-dataset validation. Hekmati et al. [18] addressed sophisticated DDoS attacks in which numerous IoT devices camouflage malicious traffic as benign. They introduced correlation-aware neural-network architectures with inter-device traffic correlations via LSTM and Transformer models. Data for experiments was taken from a 4060-node real-world IoT system. Correlation-aware LSTM test scores demonstrated 81% F1 while non-correlation-aware LSTM test scores showed 35% F1, but correlation sharing presents resource constraints.

Tseng et al. [19] tackled IoT intrusion detection from a binary and multi-class traffic classification perspective. They evaluated seven deep-learning models, including Transformer, using the CIC-IoT-2023 dataset containing 46,686,579 samples and 33 attack types. Transformer's multi-class accuracy was 99.40%, however, there may be generalization and classification efficiency issues because of class imbalance and irrelevant features.

Zhu et al. [20] addressed abnormal and encrypted IoT traffic classification by introducing the CMTSNN Deep Learning Model (CMTSNN-DL) for multi-class traffic identification. CMTSNN-DL has approximately 94.2% and 97.0% accuracy when running on the ISCX-VPN-nonVPN and ISCX-Tor2016 datasets, respectively, but the processing time and traffic diversity are limitations. Awajan [21] addressed the problem of real-time intrusion detection in IoT networks, where increasing attacks threaten connected devices. The study employed a four-layer deep fully connected neural network fed with simulated and real intrusion traffic such as Blackhole, DDoS, Opportunistic service, Sinkhole, and Wormhole attacks. It achieved 93.74% average accuracy, but further real-world scalability and generalization remain limitations.

Rafique et al. [22] addressed the growing challenge of IoT network anomaly detection by reviewing existing machine-learning and deep-learning techniques for identifying diverse attacks. The study focused on the analysis of published research and commonly used IoT datasets, and not the development of a new detection model. It pointed out that having different kinds of data sets, testing in real time, scalability, and better generalization are all significant challenges. Altaf et al. [23] addressed the difficulty of detecting sequential IoT botnet attacks by introducing a sequential gated graph convolutional network (GGCN) that models temporal network-flow relationships. Experiments used the BoT-IoT and Mirai datasets. The model gave binary accuracy of 99.97% and 99.99% respectively, but the performance was still fairly limited when considering multi-class accuracy, especially on Mirai.

Kuthadi et al. [24] addressed energy management and efficient data distribution in IoT-enabled wireless sensor networks. They have implemented an optimized energy-management framework to increase the efficiency of the network and data distribution. While the study used simulation experiments to assess the model's effectiveness in energy utilization and network performance, there is a need for more extensive real-world testing and scalability analysis. Manogaran et al. [25] addressed secure authentication and authorization in Internet of Vehicles (IoV) communication. They created a token authentication protocol for secure vehicle-to-vehicle and network communications. Experimental assessment showed that the systems could perform more securely and efficiently in communication and authentication, but there could still be some drawbacks in dealing with the computational overhead and large-scale heterogeneous IoV deployment. The existing studies are related to specific attacks, adaptive detection, transformer, graph learning, or anomaly detection, all lack unified deep malicious-traffic pattern classification for smart homes. DPC-MNT-SHE fills this gap with full representation and classification of IoT traffic.

3. Proposed Methodology

To develop DPC-MNT-SHE for learning discriminative deep traffic patterns and accurately detecting and classifying diverse malicious network traffic within IoT-based smart-home environments using RT-IoT2022.

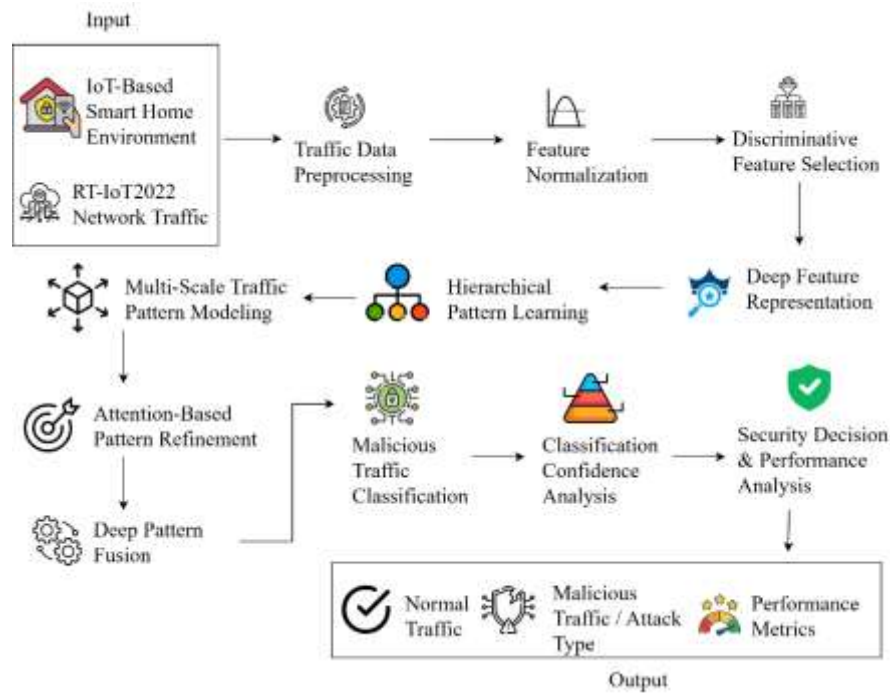


Figure 1: Overall Architecture of DPC-MNT-SHE Framework

The RT-IoT2022 dataset is a multivariate IoT network-traffic dataset containing 123,117 instances and 83 traffic features with an attack-type label [26]. It combines bidirectional flow statistics that are collected with Zeek and Flowmeter, including packet counts, flow duration, packet rates, flow payload characteristics, inter-arrival times, TCP flags, header statistics and protocol information. Both benign IoT communication and malicious activities such as DoS, DDoS, ARP poisoning, Nmap scanning and SSH bruteforcing were used in the data set. It can be used for supervised multi-class classification and Intrusion Detection in real-time IoT scenarios.

Figure 1 shows the general DPC-MNT-SHE system for the detection of malicious network traffic in smart home environments based on the IoT paradigm. RT-IoT2022 traffic containing normal and malicious patterns is first preprocessed, normalized, and filtered through discriminative feature selection. Informative traffic representations are then derived from deep feature representation, hierarchical learning, multi-scale modelling, attention-based refinement and deep pattern fusion. The classification stage classifies malicious traffic and attacks types, and the security decision generation and confidence analysis validate the predictions. Finally, performance analysis provides classification results and detection results.

3.1 Deep Traffic Pattern Representation and Learning

Equation (1) — Traffic Preprocessing and Normalization

$$X^{(n)} = \left[\frac{\mathcal{P}(x_{ij}) - \mu_j}{\sqrt{\sigma_j^2 + \epsilon}} \right]_{\substack{i=1, \dots, N \\ j=1, \dots, D}} \quad (1)$$

In this equation (1), $X^{(n)} \in \mathbb{R}^{N \times D}$ denotes the normalized traffic matrix, x_{ij} represents the j -th raw traffic feature of the i -th sample, and $\mathcal{P}(\cdot)$ denotes preprocessing operations applied to the RT-IoT2022 traffic data. Here, μ_j and σ_j^2 denote the mean and variance of feature j , respectively, while $\epsilon > 0$ is a small numerical-stability constant.

Equation (2) — Discriminative Feature Selection and Initial Representation

$$W_s^* = \arg \max_{W_s \in \mathbb{R}^{D \times d}} \frac{\text{Tr}(W_s^T S_B W_s)}{\text{Tr}(W_s^T S_W W_s) + \lambda \|W_s\|_F^2}, \quad H^{(0)} = \phi(X^{(n)} W_s^* + b_s) \quad (2)$$

In this equation (2), $W_s^* \in \mathbb{R}^{D \times d}$ denotes the optimal discriminative projection matrix, where $d < D$ is the selected feature dimension, while S_B and S_W represent the between-class and within-class scatter matrices, respectively. The variables λ and $\|W_s\|_F$ denote the regularization coefficient and Frobenius norm, while b_s is the projection bias and $\phi(\cdot)$ is the nonlinear activation function.

Equation (3) — Hierarchical Multi-Scale Traffic Pattern Learning

$$H_l^{(s)} = \phi \left(W_l^{(s)} H_{l-1}^{(s)} + U_l^{(s)} \text{Pool} \left(H_{l-1}^{(s)} \right) + b_l^{(s)} \right), \quad Z = \text{Concat}_{s=1}^S \left(H_L^{(s)} \right) \quad (3)$$

In this equation (3), $H_l^{(s)}$ denotes the learned traffic representation at hierarchical layer l and scale s , L is the number of hierarchical layers, and S is the number of traffic-pattern scales. The variables $W_l^{(s)}$ and $U_l^{(s)}$ are learnable transformation matrices, $b_l^{(s)}$ is the corresponding bias, $\text{Pool}(\cdot)$ denotes the pooling operation, and $\text{Concat}(\cdot)$ produces the combined multi-scale representation Z .

3.2 Malicious Traffic Classification and Security Decision Analysis

Equation (4) — Attention-Based Pattern Refinement and Fusion

$$e_t^{(h)} = v_h^T \tanh(W_h z_t + b_h), \alpha_t^{(h)} = \frac{\exp(e_t^{(h)})}{\sum_{k=1}^T \exp(e_k^{(h)})}, \tilde{z}_t = \text{Concat}_{h=1}^H \left(\alpha_t^{(h)} V_h z_t \right), F = \text{Concat}_{t=1}^T (\tilde{z}_t) \quad (4)$$

In this equation (4), z_t denotes the t -th feature vector of the multi-scale representation Z , T denotes the number of feature positions, and H denotes the number of attention heads. The variables W_h , V_h , v_h , and b_h are learnable attention parameters, $e_t^{(h)}$ is the attention score, $\alpha_t^{(h)}$ is the normalized attention weight, and F denotes the fused deep traffic representation.

Equation (5) — Malicious Traffic Classification and Confidence Estimation

$$p_i = \text{Softmax}(W_c F_i + b_c), p_{ic} = \frac{\exp(w_c^T F_i + b_c)}{\sum_{j=1}^C \exp(w_j^T F_i + b_j)}, \hat{y}_i = \arg \max_{c \in \{1, \dots, C\}} p_{ic}, \Gamma_i = \max_c p_{ic} \quad (5)$$

In this equation (5), F_i denotes the fused representation of traffic sample i , C denotes the number of traffic classes, and W_c and b_c denote the classifier weight matrix and bias vector. The variables p_{ic} , w_c , and b_c denote the probability, weight vector, and bias associated with class c , while $\hat{y}_i$ denotes the predicted class and Γ_i denotes the maximum classification confidence.

Algorithm 1: DPC-MNT-SHE

1. **Input:** $X_{RT} \in \mathbb{R}^{N \times D}$;
2. **Output:** $\hat{Y}, \mathcal{D}, \mathcal{M}$;
3. initialize ϵ, λ, τ .
4. $X^{(p)} \leftarrow \mathcal{P}(X_{RT})$;
5. **for** $i = 1, \dots, N$ **do** $x_i \leftarrow \mathcal{P}(x_i)$; **end for**.
6. $X_{ij}^{(n)} \leftarrow \frac{X_{ij}^{(p)} - \mu_j}{\sqrt{\sigma_j^2 + \epsilon}}$;

```

7. for  $j = 1, \dots, D$  do
8.   compute  $\mu_j, \sigma_j^2$ ; end for.
9.    $W_s^* \leftarrow \arg \max_{W_s} \frac{\text{Tr}(W_s^T S_B W_s)}{\text{Tr}(W_s^T S_W W_s) + \lambda \|W_s\|_F^2}$ ;  $H^{(0)} \leftarrow \phi(X^{(n)} W_s^* + b_s)$ 
10.  for  $l = 1, \dots, L$  do
11.     $H_l \leftarrow \phi(W_l H_{l-1} + b_l)$ ;
12.  end for.
13.  for  $s = 1, \dots, S$  do
14.     $H_l^{(s)} \leftarrow \phi(W_l^{(s)} H_{l-1}^{(s)} + U_l^{(s)} \text{Pool}(H_{l-1}^{(s)}) + b_l^{(s)})$ ;
15.  end for;
16.   $Z \leftarrow \text{Concat}_{s=1}^S H_L^{(s)}$ .
17.  while  $t \leq T$  do  $\alpha_t^{(h)} \leftarrow \frac{e^{e_t^{(h)}}}{\sum_{k=1}^T e^{e_k^{(h)}}}$ ;
18.     $\tilde{z}_t \leftarrow \text{Concat}_{h=1}^H (\alpha_t^{(h)} \mathbf{V}_h \mathbf{z}_t)$ ;  $t \leftarrow t + 1$ ;
19.  end while.
20.   $F \leftarrow \text{Concat}_{t=1}^T \tilde{z}_t$ ;
21.  while  $i \leq N$  do
22.     $p_i \leftarrow \text{Softmax}(W_c F_i + b_c)$ ;  $\hat{y}_i \leftarrow \arg \max_c p_{ic}$ ;  $\Gamma_i \leftarrow \max_c p_{ic}$ ;  $i \leftarrow i + 1$ ;
23.  end while.
24.  for  $i = 1, \dots, N$  do
25.    if  $\Gamma_i < \tau$  then  $\mathcal{D}_i \leftarrow \text{Uncertain}$ ; else if  $\hat{y}_i = \text{Normal}$  then  $\mathcal{D}_i \leftarrow \text{Normal}$ ; else
       $\mathcal{D}_i \leftarrow \text{Malicious}(\hat{y}_i)$ ;
26.    end if;
27.  end for.
28.   $\text{Acc} = \frac{TP+TN}{TP+TN+FP+FN}$ ,  $P = \frac{TP}{TP+FP}$ ,  $R = \frac{TP}{TP+FN}$ ,  $F1 = \frac{2PR}{P+R}$ ;
29.  return  $(\hat{\mathbf{Y}}, \mathcal{D}, \mathcal{M})$ .

```

Algorithm 1 presents the DPC-MNT-SHE framework for IoT malicious-traffic detection. It receives RT-IoT2022 traffic data, normalize it, selects discriminative features, learn hierarchical and multi-scale patterns, refine their attention, fuse features, classify them, assess their confidence, make a security decision and evaluate their performance to return confident traffic predictions.

4. Results and Discussion

Table 1 shows the experimental setup and the hyperparameters of DPC-MNT-SHE such as dataset splitting, training, software platform, run time platform, IoT clients and GPU powered server infrastructure.

Table 1: *Experimental Setup and Hyperparameter Configuration for the DPC-MNT-SHE framework*

Component	Configuration
Dataset	RT-IoT2022 [26]
Training/Testing Split	80% / 20%
Optimizer	Adam
Learning Rate	0.001

Batch Size	64
Epochs	100
Dropout Rate	0.30
Activation Function	ReLU
Loss Function	Categorical Cross-Entropy
Software	Python 3.10, TensorFlow/Keras, Scikit-learn
Runtime	Google Colab / Jupyter Notebook
Clients	IoT smart-home traffic sources
Server	GPU-enabled computational server

4.1 Accuracy (%)

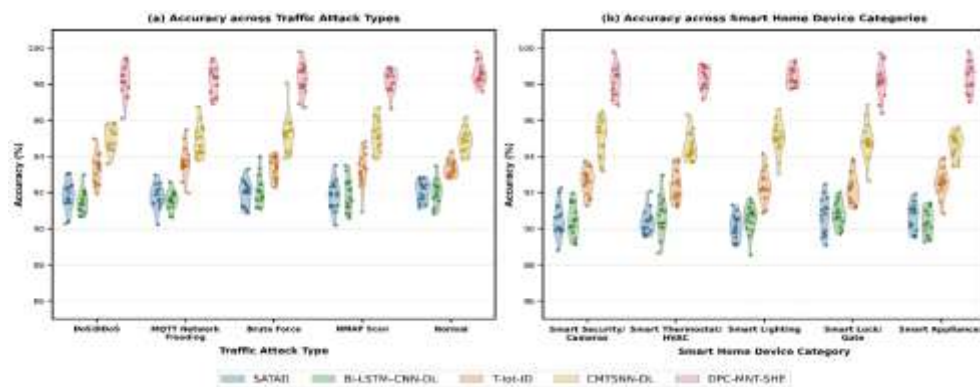


Figure 2: Accuracy (%)

In Figure 2, (a) evaluates the accuracy across different traffic attack types, while (b) demonstrates performance stability across smart home device categories. In all conditions under evaluation, the proposed DPC-MNT-SHE method shows consistently the highest accuracy when compared with other models.

4.2 Precision (%)

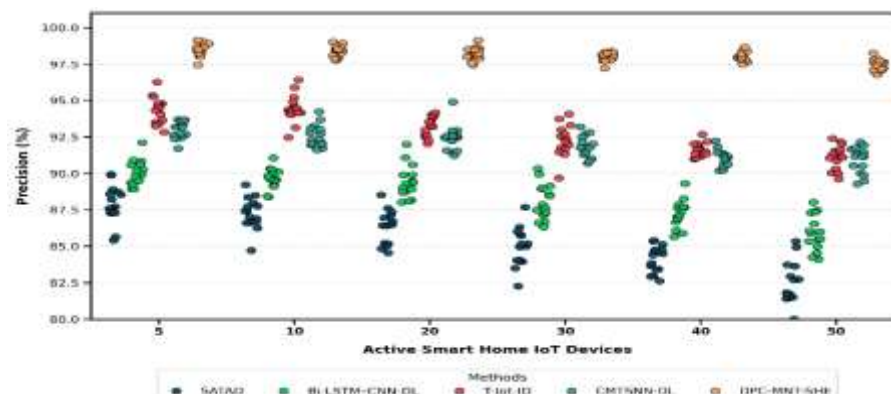


Figure 3: Precision (%)

Figure 3 shows that the evaluation is able to achieve precision performance under different number of active smart home IoT devices. The proposed DPC-MNT-SHE method is able to obtain the highest precision in comparison with the other evaluated methods for all the densities in the range of 5-50 active devices in a network.

4.3 Recall (%)

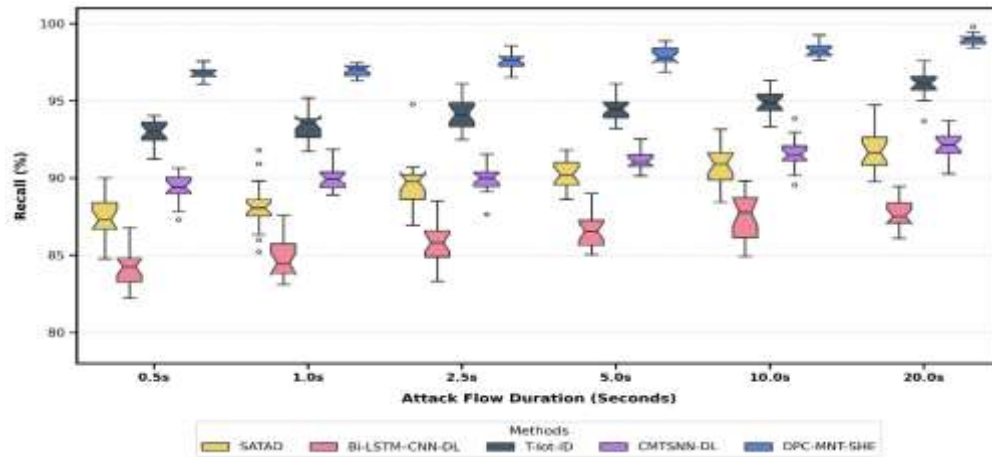


Figure 4: Recall (%)

In Figure 4 the assessment shows the recall performance for growing durations of attack flow in seconds. The length of the attack duration gradually increases from 0.5s to 20.0s, and the proposed DPC-MNT-SHE model results in recall at the highest level for all tested models.

4.4 F1-Score (%)

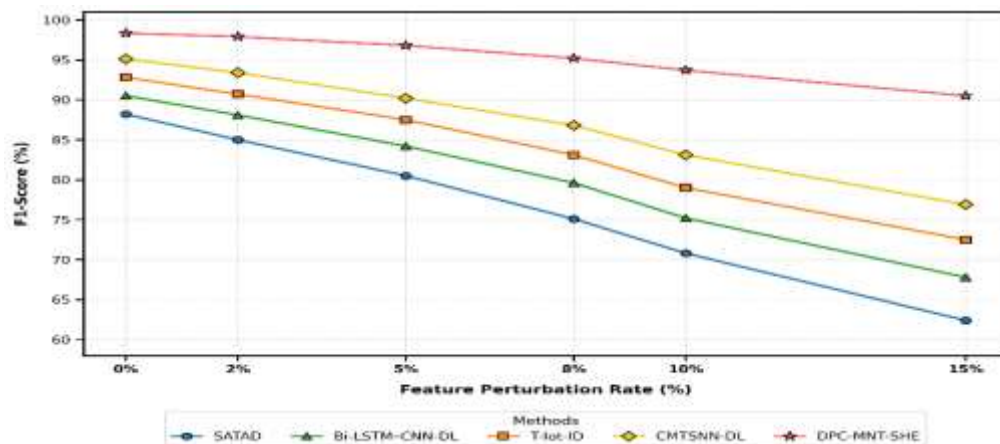


Figure 5: F1-Score (%)

In Figure 5, the evaluation shows robustness of the F1-Score with increased feature perturbation levels (0%–15%). All models experience performance loss as data distortion increases; however, the proposed DPC-MNT-SHE method consistently obtains high F1-Score among all the models evaluated.

Table 2 shows the accuracy, precision, recall, and F1-score of DPC-MNT-SHE against other methods, and results indicate that the overall malicious traffic classification performance of DPC-MNT-SHE is superior in the analyzed IoT smart-home traffic scenarios.

Table 2: Performance Comparison of Proposed and Existing Methods.

<i>Method</i>	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
<i>SATAD</i>	91.8	91.2	90.9	91.0
<i>Bi-LSTM–CNN-DL</i>	94.6	94.3	94.1	94.2
<i>T-IoT-ID</i>	95.4	95.1	94.8	94.9
<i>CMTSNN-DL</i>	96.2	96.0	95.8	95.9
<i>DPC-MNT-SHE</i>	98.5	98.6	96.5	98.35

Table 3 presents the ablation study, showing that removing individual components reduces performance. The results of the DPC-MNT-SHE model show that it gains the most overall accuracy, precision, recall, and F1-score, which shows that the integrated components have contributed to the final results of the DPC-MNT-SHE model.

Table 3: Ablation Study

<i>Model Configuration</i>	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
<i>Without Feature Selection</i>	95.8	95.5	95.2	95.3
<i>Without Hierarchical Pattern Learning</i>	96.4	96.1	95.9	96.0
<i>Without Attention-Based Refinement</i>	97.1	96.8	96.6	96.7
<i>Without Deep Pattern Fusion</i>	97.6	97.3	97.1	97.2
<i>DPC-MNT-SHE (Full Model)</i>	98.5	98.6	96.5	98.35

5. Conclusion

The proposed DPC-MNT-SHE framework effectively addresses malicious network traffic detection in IoT-based smart-home environments by integrating preprocessing, feature representation, deep pattern learning, and multi-class classification. It showed reliable classification performance with 98.5% accuracy, 98.6% precision, 96.5% recall, and 98.35% F1-score on the RT-IoT2022 dataset. However, the study is limited by its evaluation on a single dataset and the computational requirements associated with deep learning. Future work will focus on cross-dataset validation, real-time deployment on resource-constrained IoT, adaptive learning for evolving attack patterns, and lightweight model optimization to improve scalability, robustness, and practical applicability across heterogeneous smart-home networks.

REFERENCES

- [1]. Rauf Ali Khan, M., Barnawi, A. Y., Munir, A., Als Salman, Z., & Satan Sanunga, D. M. (2025). Lightweight quantized XGBoost for botnet detection in resource-constrained IoT networks. *IoT*, 6(4), 70.
- [2]. Altulaihah, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors*, 24(2), 713.
- [3]. Keleşoğlu, N., & Sobczak, Ł. (2024). Zigbeenet: Decrypted zigbee iot network traffic dataset in smart home environment. *Applied Sciences*, 14(23), 10844.
- [4]. Elayan, A., & Kadoch, M. (2026). Enhancing IoT network security: A BPSO-optimized attention-GRU deep learning framework for intrusion detection. *Computers*, 15(5), 266.
- [5]. Liu, M., Yang, Q., Wang, W., & Liu, S. (2024). Semi-supervised encrypted malicious traffic detection based on multimodal traffic characteristics. *Sensors*, 24(20), 6507.
- [6]. Shalan, M., Hasan, M. R., Bai, Y., & Li, J. (2025). Enhancing smart home security: Blockchain-enabled federated learning with knowledge distillation for intrusion detection. *Smart Cities*, 8(1), 35.
- [7]. Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S., & Dhaou, I. B. (2023). Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model. *IEEE Access*, 11, 119862-119875.
- [8]. Seyedi, B., & Postolache, O. (2025). Securing IoT communications via anomaly traffic detection: synergy of genetic algorithm and ensemble method. *Sensors*, 25(13), 4098.
- [9]. Al-Fawa'reh, M., Abu-Khalaf, J., Szewczyk, P., & Kang, J. J. (2023). MalBoT-DRL: Malware botnet detection using deep reinforcement learning in IoT networks. *IEEE Internet of Things Journal*, 11(6), 9610-9629.
- [10]. O. A. M. Z. A. L. Shamsi, (2026). Federated Graph Neural Pattern Learning Framework for Adaptive Intrusion Detection in Large-Scale IoT Networks. *PatternIQ Mining (PIQM)*, 3(1), 175-194. <https://doi.org/10.70023/piqm3110>
- [11]. Anitha, T., Aanjankumar, S., Poonkuntran, S., & Nayyar, A. (2023). A novel methodology for malicious traffic detection in smart devices using BI-LSTM-CNN-dependent deep learning methodology. *Neural Computing and Applications*, 35(27), 20319-20338.
- [12]. Watanabe, N., Yamazaki, T., Miyoshi, T., Yamamoto, R., Nakahara, M., Okui, N., & Kubota, A. (2024). Self-adaptive traffic anomaly detection system for IoT smart home environments. *IEICE Transactions on Communications*, 108(3), 230-242.
- [13]. Wang, M., Yang, N., & Weng, N. (2023). Securing a smart home with a transformer-based IoT intrusion detection system. *Electronics*, 12(9), 2100.
- [14]. Abdusalomov, A., Kilichev, D., Nasimov, R., Rakhmatullayev, I., & Im Cho, Y. (2024). Optimizing smart home intrusion detection with harmony-enhanced extra trees. *IEEE Access*, 12, 117761-117786.
- [15]. Reis, M. J. (2025). Edge-FLGuard+: A federated and lightweight anomaly detection framework for securing 5G-enabled IoT in smart homes. *Future Internet*, 17(8), 329.
- [16]. Reis, M. J., & Serôdio, C. (2025). Edge AI for real-time anomaly detection in smart homes. *Future Internet*, 17(4), 179.
- [17]. Wahab, S. A., Sultana, S., Tariq, N., Mujahid, M., Khan, J. A., & Mylonas, A. (2025). A multi-class intrusion detection system for DDoS attacks in IoT networks using deep learning and transformers. *Sensors*, 25(15), 4845.
- [18]. Hekmati, A., Zhang, J., Sarkar, T., Jethwa, N., Grippo, E., & Krishnamachari, B. (2024). Correlation-aware neural networks for DDoS attack detection in IoT systems. *IEEE/ACM transactions on networking*, 32(5), 3929-3944.
- [19]. Tseng, S. M., Wang, Y. Q., & Wang, Y. C. (2024). Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset. *Future Internet*, 16(8), 284.
- [20]. Zhu, S., Xu, X., Gao, H., & Xiao, F. (2023). CMTSNN: A deep learning model for multiclassification of abnormal and encrypted traffic of Internet of Things. *IEEE Internet of Things Journal*, 10(13), 11773-11791.
- [21]. Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers*, 12(2), 34.

- [22]. Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends. *Sensors*, 24(6), 1968.
- [23]. Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. P., & Braun, R. (2024). GNN-based network traffic analysis for the detection of sequential attacks in IoT. *Electronics*, 13(12), 2274.
- [24]. Kuthadi, V. M., Selvaraj, R., Baskar, S., Shakeel, P. M., & Ranjan, A. (2022). Optimized energy management model on data distributing framework of wireless sensor network in IoT system. *Wireless Personal Communications*, 127(2), 1377–1403.
- [25]. Manogaran, G., Rawal, B. S., Saravanan, V., M. K., P., Xin, Q., & Shakeel, P. (2023). Token-based authorization and authentication for secure Internet of Vehicles communication. *ACM Transactions on Internet Technology*, 22(4), 1–20.
- [26]. Supplejade. (2023). RT-IoT2022: Real-time Internet of Things [Data set]. Kaggle. <https://www.kaggle.com/datasets/supplejade/rt-iot2022real-time-internet-of-things>