**Bulletin of Electrical Engineering and Informatics**
Vol. 15, No. 6, December 2026, pp. 5438~5449
ISSN: 2302-9285, DOI: 10.11591/eei.v15i6.14022 

# Semantic group network learning for enterprise and internet of things intrusion detection

**Sivakumaran Arumugam[1], Sumithra Mani[2], Anbarasu Rajabather[3], Rajesh Elangovan[4], Arshita Srivastava[5], Prabhakaran Rajkumar[6]**
[1]Department of Computer Science and Engineering (Artificial Intelligence), RMK College of Engineering and Technology, Chennai, India
[2]Department of Information Technology, Panimalar Engineering College, Chennai, India
[3]Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, India
[4]Department of Information Technology, Alliance School of Advanced Computing, Alliance University, Bengaluru, India
[5]Department of Computer Science and Applications, Sharda School of Computing Science and Engineering, Sharda University, Greater Noida, India
[6]Faculty of Computer Science and Information Technology, Vel Tech Multi Tech Engineering College, Chennai, India

**Article Info**

***Article history:***

Received Jul 19, 2026
Revised Sep 12, 2026
Accepted Oct 4, 2026

***Keywords:***

Behavioral learning
Enterprise networks
Intrusion detection
Network security
Semantic feature grouping
Semantic representation learning

**ABSTRACT**

Conventional intrusion detection models learn directly from individual network flow attributes, making their performance susceptible to variations in traffic characteristics across enterprise and internet of things (IoT) environments. To address this limitation, this paper proposes a semantic group network-based intrusion detection system (SGNet-IDS), a semantic group network learning framework that models network behavior through structured semantic representations rather than isolated features. The framework organizes normalized flow attributes into five semantic behavioral groups and employs a semantic group interaction module (SGIM) to capture complementary relationships among communication characteristics, producing compact latent representations for intrusion classification. SGNet-IDS was evaluated on the CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 datasets and compared with representative intrusion detection methods and stronger tabular learning baselines. The proposed framework achieved 99.71% and 99.00% accuracy, with micro-averaged F1-scores of 99.14% and 99.48%, respectively. Ablation analysis demonstrated that semantic grouping and interaction learning each contributed to the overall detection performance, while computational evaluation confirmed competitive inference efficiency with moderate model complexity. These results indicate that SGNet-IDS provides an effective and computationally efficient semantic representation framework for intrusion detection across heterogeneous enterprise and IoT network environments.

*This is an open access article under the CC BY-SA license.*

***Corresponding Author:***

Rajesh Elangovan
Department of Information Technology, Alliance School of Advanced Computing, Alliance University
Bengaluru, Karnataka, India
Email: rajesh.e@alliance.edu.in

## 1. INTRODUCTION

Network intrusion detection has become increasingly challenging as enterprise infrastructures and internet of things (IoT) deployments continue to converge [1]. Enterprise networks are typically characterized by high-throughput communication, stable infrastructure, and standardized protocols, whereas IoT environments consist of heterogeneous devices generating lightweight, burst-oriented, and application-specific

traffic [2], [3]. Although these environments differ considerably in communication behavior, both are exposed to similar cyber threats, including denial-of-service (DoS) attacks, reconnaissance, brute-force attempts, botnet activity, and protocol exploitation [4], [5]. As organizations increasingly integrate enterprise services with IoT platforms, intrusion detection systems (IDSs) are expected to operate reliably across network environments that exhibit substantially different traffic characteristics [6].

Machine learning and deep learning have significantly improved the capability of IDSs to identify malicious traffic [7], [8]. Recent studies have reported excellent detection accuracy by combining sophisticated feature engineering with increasingly complex learning architectures [9], [10]. Nevertheless, many published methods remain closely coupled to the statistical properties of the datasets used during training [11], [12]. As a result, improvements observed on benchmark datasets do not always translate into stable performance when traffic characteristics change across deployment environments [13], [14]. This limitation is particularly evident when enterprise-trained models are applied to IoT traffic, where differences in communication frequency, packet distribution, protocol usage, and device behavior introduce substantial variations in feature distributions [15], [16].

Recent research has explored different directions to improve network intrusion detection. Alkadi *et al.* [17] investigated multiple machine learning algorithms for IoT intrusion detection and demonstrated that careful preprocessing and model selection substantially influence detection performance. Awajan [18] proposed a protocol-independent deep learning framework combining anomaly detection with fully connected neural networks to support real-time IoT security. Hnamte and Hussain [19] integrated convolutional and recurrent neural networks to exploit spatial and sequential traffic characteristics, achieving high accuracy on benchmark datasets. Although these studies reported competitive results, their evaluations remained primarily confined to individual datasets, providing limited evidence regarding the robustness of learned feature representations across heterogeneous network environments.

Several researchers have subsequently recognized the importance of cross-dataset evaluation. Cantone *et al.* [20] systematically examined model transferability across multiple intrusion detection datasets and reported significant performance degradation despite excellent in-dataset accuracy. Oliveira *et al.* [21] introduced a distributed ensemble framework to improve scalability and cross-dataset capability, while Wang *et al.* [22] proposed Learn-IDS to reduce distribution mismatch through unified preprocessing and dataset engineering. These studies demonstrated that dataset diversity directly affects model reliability; however, their primary emphasis remained on framework integration, sampling strategies, or deployment architecture rather than on improving the underlying feature representation itself.

Feature engineering has also received considerable attention. Raza *et al.* [23] combined conventional machine learning with deep learning models for enterprise and IoT intrusion detection, whereas Lin *et al.* [24] enhanced extreme learning machine (ELM) through multi-feature extraction for cloud-based IoT security. More *et al.* [25] demonstrated that correlation-based feature selection effectively reduces redundant attributes, improving detection performance on UNSW-NB15. These approaches confirm that feature quality strongly influences classification accuracy; however, they generally treat individual flow features as independent variables or rely on statistical importance measures during feature selection. Consequently, relationships among behaviorally related network characteristics are often only implicitly represented within the learning model.

Another active research direction focuses on handling evolving traffic behavior. Shyaa *et al.* [26] introduced reinforcement learning and incremental learning strategies to address feature drift, while Yang *et al.* [27] developed a representation adaptation framework for concept drift using self-supervised learning. Chu *et al.* [28] proposed an ensemble-based drift localization mechanism for streaming IoT environments, and Noori *et al.* [29] investigated dynamic feature-aware ensemble learning for evolving data streams. Although these methods improve adaptability under changing traffic conditions, they primarily concentrate on updating models after drift occurs instead of strengthening the semantic representation learned from network traffic before classification.

A common characteristic of most existing IDS frameworks is that the learning process begins directly from individual flow attributes after normalization or feature selection. Features describing related network behaviors-for example, traffic intensity, temporal activity, packet statistics, transport behavior, and directional communication-are usually processed independently even though they collectively describe the same underlying communication pattern. Learning from isolated features may obscure complementary behavioral relationships and increase sensitivity to variations in feature distributions between enterprise and IoT environments. Organizing related features into behavior-oriented semantic groups provides an opportunity to construct more structured traffic representations while preserving the relationships among complementary network characteristics.

Motivated by this observation, this paper presents semantic group network learning for intrusion detection across enterprise and IoT traffic (SGNet-IDS). Rather than emphasizing classifier complexity, SGNet-IDS introduces a semantic representation strategy in which network flow attributes are first organized

into behavior-oriented semantic groups. Interactions among these groups are subsequently modeled through a semantic group interaction module (SGIM) to generate compact latent representations before the final classification stage. By separating behavioral representation learning from decision making, the proposed framework seeks to reduce dependence on individual feature distributions while improving discrimination between benign and malicious traffic across heterogeneous network environments.

The main contributions of this work are summarized as follows:

- A domain-guided semantic behavioral representation strategy is proposed to organize flow-based network features into behavior-oriented groups, providing a structured alternative to direct feature-level representation learning.
- An SGIM is introduced to explicitly model pairwise relationships among compact behavioral group representations and incorporate these relationships into the latent intrusion-detection representation.
- A unified experimental evaluation is conducted using the CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 datasets under a consistent preprocessing framework to assess the applicability of SGNet-IDS across enterprise and IoT traffic.
- Comprehensive comparative and ablation analyses demonstrate that semantic group learning improves intrusion detection performance while maintaining computational efficiency suitable for practical deployment.

The remainder of this paper is organized as follows. Section 2 presents the proposed SGNet-IDS framework, including semantic feature grouping and interaction learning. Section 3 describes the experimental setup and reports the comparative evaluation and discusses the findings, and section 4 concludes the paper.

## 2. METHOD

### 2.1. Overview of semantic group network-based intrusion detection system

Intrusion detection models are commonly trained using individual flow attributes [6], allowing each feature to contribute independently to the learning process. Although this representation is effective for in-dataset classification, it often overlooks the behavioral relationships among network characteristics describing the same communication activity. Features associated with packet statistics, traffic intensity, temporal dynamics, or transport behavior are therefore treated as isolated variables, even though they collectively characterize a single network event. SGNet-IDS addresses this limitation by introducing semantic group learning as the primary representation mechanism. Instead of directly processing normalized feature vectors, the proposed framework first organizes correlated network attributes into semantic behavioral groups. Each group captures a distinct aspect of network communication, while the interaction among groups forms a compact representation describing the overall traffic behavior. The framework consists of five sequential stages: feature normalization, semantic grouping, semantic interaction learning, latent behavior embedding, and intrusion classification. Figure 1 illustrates the complete workflow.

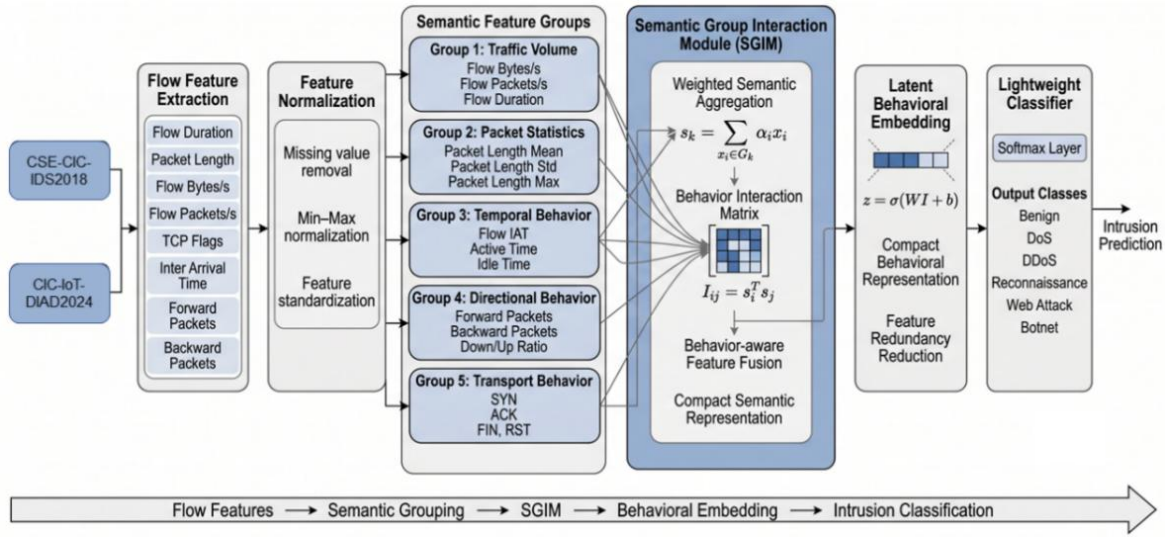



Figure 1. Overall architecture of the proposed SGNet-IDS framework

Unlike conventional feature selection methods that remove low-ranked attributes, semantic grouping preserves all behaviorally relevant information while reducing the dependence on individual feature distributions. This representation enables the classifier to learn network behavior from complementary semantic patterns rather than isolated measurements.

### 2.2. Semantic feature group construction

Let the normalized network flow be represented by

$$X = [x_1, x_2, \dots, x_n]$$

where $n$ denotes the total number of flow features. Rather than processing the normalized feature vector directly, SGNet-IDS organizes the flow features into $K$ predefined semantic groups according to their communication semantics (1):

$$G = \{G_1, G_2, \dots, G_K\} \quad (1)$$

where each semantic group represents a specific communication characteristic, including traffic volume, packet statistics, temporal behavior, directional communication, and transport behavior [15]. In this work, $K$=5, corresponding to traffic volume, packet statistics, temporal behavior, directional communication, and transport behavior. Grouping is performed according to feature semantics rather than statistical importance, allowing related network attributes to remain structurally connected throughout the learning process.

The predefined grouping represents a domain-guided structural prior rather than conventional manual feature selection. The original flow attributes are retained and organized according to their underlying communication behavior, without ranking or discarding features. This organization defines the behavioral units for subsequent representation learning, while the contribution of individual features within each group is learned adaptively through the weighted aggregation in (2). Thus, the semantic grouping provides the structural organization, whereas the feature contributions and subsequent group interactions remain data-driven. The specific feature assignments used for the five groups are illustrated in Figure 1.

### 2.3. Semantic group representation

After constructing the semantic groups, each group is transformed into a compact behavioral representation through a learnable weighted aggregation. Rather than assigning equal importance to all features, SGNet-IDS estimates the contribution of each feature within its corresponding semantic group [8], allowing behaviorally informative traffic characteristics to contribute more strongly to the final representation. For the $k^{th}$ semantic group, the semantic representation is computed as (2):

$$\mathrm{s_k} = \sum_{x_i \in G_k} \alpha_i \, x_i, \text{ where } \sum_{x_i \in G_k} \alpha_i = 1 \quad (2)$$

The weighting coefficients are normalized through a softmax operation during model optimization, ensuring that their contributions sum to one within each semantic group. Where, $G_k$ denotes the $k^{th}$ semantic feature group, $x_i$ is the normalized feature belonging to $G_k$, $\alpha_i$ represents the learnable importance weight assigned to feature $x_i$, and $s_k$ is the semantic representation of the corresponding behavioral group. During model optimization, these coefficients are learned automatically to emphasize behaviorally informative features while suppressing redundant or less discriminative attributes. Consequently, each semantic representation captures the dominant communication characteristics of its behavioral group without requiring manual feature selection. Unlike conventional feature weighting methods that estimate feature importance globally, the proposed aggregation operates within each semantic behavioral group, preserving complementary relationships among behaviorally related network attributes. Consequently, SGNet-IDS constructs behavioral representations that emphasize relationships among related network characteristics rather than relying exclusively on individual feature contributions.

### 2.4. Semantic group interaction module

After semantic representations are generated, SGNet-IDS models the interactions among behavioral groups using the proposed SGIM. The interaction score between two semantic groups is defined as (3):

$$I_{ij} = \mathrm{s_i^T s_j} \quad (3)$$

where $\mathrm{s_i}$ and $\mathrm{s_j}$ denote the semantic representations of the $i^{th}$ and $j^{th}$ behavioral groups, respectively.

The interaction operation in (3) uses a conventional dot-product similarity [12]; therefore, its novelty does not arise from the mathematical operator itself. Instead, SGIM applies this operation to the learned representations of semantically defined behavioral groups. Each interaction element consequently represents a relationship between two communication behaviors rather than between isolated raw features. With $K$=5 groups, SGIM produces a compact $K \times K$ behavioral interaction matrix, which is subsequently integrated with the group representations. This design separates feature aggregation from behavioral interaction learning and explicitly represents cross-behavior relationships for intrusion detection.

Pairwise interaction scores are computed for all semantic group pairs to construct the interaction matrix $I = [I_{ij}] \in R^{K \times K}$, summarizing the complementary relationships among the behavioral groups. The predefined structure determines the behavioral units summarized before interaction learning, while the interaction strengths are learned from the data. Thus, SGIM does not claim novelty in the dot-product operation itself; rather, its methodological distinction lies in applying a simple interaction operator to compact, behavior-oriented representations instead of individual raw features or the complete feature space.

The contribution of SGIM is further supported by the ablation results. Removing SGIM reduces accuracy from 99.71% to 99.34% and F1-score from 99.14% to 98.54%, indicating that explicitly modeling relationships among semantic group representations provides additional discriminative information beyond semantic aggregation alone.

### 2.5. Latent behavioral embedding

The interaction matrix is transformed into a compact latent representation (4):

$$\mathrm{z} = \sigma(WI + b) \tag{4}$$

where $W$ is the projection matrix, $b$ is the bias vector, $\sigma(\cdot)$ denotes the rectified linear unit (ReLU) activation function, and z represents the latent behavioral embedding.

This embedding summarizes the joint communication behavior of each network flow while substantially reducing feature redundancy. The latent embedding preserves only the behaviorally discriminative information required for intrusion classification, thereby reducing feature redundancy and model complexity.

### 2.6. Intrusion classification

The latent embedding is finally mapped to the attack classes through a lightweight classifier. The predicted probability is computed as (5):

$$\hat{y} = Softmax\,(W_c \mathrm{z} + b_c) \tag{5}$$

where $W_c$ denotes the classification weights, $b_c$ represents the bias term, and $\hat{y}$ is the predicted class probability vector.

Model parameters are optimized using categorical cross-entropy during training. Since semantic interaction learning produces a compact behavioral representation, intrusion classification can be performed using a lightweight softmax classifier without introducing additional architectural complexity. Consequently, the primary contribution of SGNet-IDS lies in semantic representation learning rather than classifier complexity, enabling the framework to remain computationally efficient while maintaining high detection performance.

## 3. RESULTS AND DISCUSSION

The effectiveness of SGNet-IDS was evaluated on the CSE-CIC-IDS2018 [30] and CIC-IoT-DIAD2024 [31] datasets to assess its generalization across enterprise and IoT network environments. Both datasets were partitioned using a stratified 70:10:20 training, validation, and testing strategy to preserve the original class distributions. The proposed framework and all baseline methods were trained under identical experimental settings. Performance was evaluated using accuracy, precision, recall, specificity, F1-score, and receiver operating characteristic-area under the curve (ROC-AUC).

Table 1 summarizes the characteristics of the datasets used in this study. CSE-CIC-IDS2018 represents enterprise network traffic comprising multiple contemporary attack categories, whereas CIC-IoT-DIAD2024 contains heterogeneous IoT communication generated by diverse devices and attack scenarios. The two datasets differ substantially in network characteristics, attack diversity, and class distribution, enabling a comprehensive evaluation of SGNet-IDS under both conventional enterprise networks and highly imbalanced IoT environments.

Table 1. Characteristics of the datasets used for experimental evaluation

| Dataset | Network environment | Total samples | Benign samples | Attack categories | No. of classes | Class distribution |
|---|---|---|---|---|---|---|
| CSE-CIC-IDS2018 | Enterprise network | 16,232,943 | 13,484,708 | 6 | 14 | Moderately imbalanced |
| CIC-IoT-DIAD2024 | IoT network | 12,267,935 | 398,330 | 7 | 14 | Highly imbalanced |

Table 2 presents the experimental configuration and hyperparameter settings used throughout the study. A common training protocol, optimization strategy, and evaluation criteria were adopted for both datasets to ensure a fair and consistent comparison between SGNet-IDS and the baseline methods.

Table 2. Experimental configuration and hyperparameter settings of SGNet-IDS

| Category | Configuration |
|---|---|
| Datasets | CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 |
| Data split | 70% training, 10% validation, and 20% testing (stratified) |
| Feature normalization | Min-Max normalization |
| Semantic groups | 5 (traffic volume, packet statistics, temporal behavior, directional behavior, and transport behavior) |
| Optimizer | Adam |
| Initial learning rate | 0.001 |
| Batch size | 256 |
| Maximum epochs | 100 |
| Activation functions | ReLU (embedding) and softmax (output layer) |
| Loss function | Categorical cross-entropy |
| Weight initialization | Glorot (Xavier) uniform |
| Early stopping | Patience=8 (validation loss) |
| Evaluation metrics | Accuracy, precision, recall, specificity, F1-score, and ROC-AUC |
| Software environment | Python 3.11, TensorFlow, and Scikit-learn |
| Hardware platform | Intel Core i7 CPU, NVIDIA RTX 4060 (8 GB), 32 GB RAM, and Windows 11 |

Table 3 compares SGNet-IDS with conventional IDS approaches and stronger tabular learning baselines, including XGBoost, LightGBM, and FT-Transformer. Among the competing methods, FT-Transformer provides the strongest overall performance. Nevertheless, SGNet-IDS achieves the highest accuracy, precision, recall, specificity, and F1-score on both datasets. Compared with FT-Transformer, SGNet-IDS improves F1-score by 0.36 and 0.28 percentage points on CSE-CIC-IDS2018 and CIC-IoT-DIAD2024, respectively, while also achieving higher recall by 0.39 and 0.54 percentage points. The consistently lower standard deviations of SGNet-IDS further indicate stable performance across repeated runs. These results demonstrate that the proposed semantic behavioral representation remains competitive against strong tree-based and deep tabular learning approaches.

For a stronger tabular-learning comparison, XGBoost, LightGBM, and FT-Transformer were evaluated using the same input features, preprocessing procedure, data partitions, and evaluation protocol as SGNet-IDS, without applying the proposed semantic grouping and SGIM components.

Table 3. Performance (micro-average) comparison of SGNet-IDS with representative intrusion detection methods on the CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 datasets

| Method | CSE-CIC-IDS2018 | | | | | CIC-IoT-DIAD2024 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Accuracy | Precision | Recall | Specificity | F1-score | Accuracy | Precision | Recall | Specificity | F1-score |
| CNN-LSTM | 99.12±0.16 | 96.71±0.28 | 98.16±0.25 | 99.32±0.14 | 97.43±0.23 | 95.14±0.35 | 99.89±0.04 | 95.08±0.38 | 96.89±0.26 | 97.43±0.22 |
| MFE-ELM | 99.27±0.19 | 97.27±0.26 | 98.45±0.23 | 99.44±0.15 | 97.86±0.21 | 96.72±0.32 | 99.90±0.03 | 96.71±0.34 | 97.00±0.24 | 98.28±0.19 |
| XGBoost | 99.36±0.12 | 97.68±0.18 | 98.61±0.16 | 99.51±0.10 | 98.14±0.14 | 97.41±0.21 | 99.90±0.02 | 97.38±0.23 | 97.15±0.18 | 98.62±0.13 |
| LightGBM | 99.41±0.11 | 97.85±0.17 | 98.70±0.15 | 99.56±0.09 | 98.27±0.13 | 97.65±0.20 | 99.91±0.02 | 97.62±0.22 | 97.24±0.17 | 98.75±0.12 |
| Learn-IDS | 99.49±0.10 | 98.15±0.15 | 98.82±0.14 | 99.62±0.08 | 98.49±0.12 | 98.03±0.17 | 99.91±0.02 | 98.05±0.19 | 97.39±0.15 | 98.97±0.11 |
| FT-Transformer | 99.58±0.09 | 98.42±0.13 | 99.15±0.11 | 99.68±0.07 | 98.78±0.10 | 98.47±0.14 | 99.92±0.02 | 98.49±0.16 | 97.68±0.12 | 99.20±0.09 |
| **SGNet-IDS** | **99.71±0.05** | **98.74±0.09** | **99.54±0.06** | **99.74±0.04** | **99.14±0.07** | **99.00±0.08** | **99.94±0.01** | **99.03±0.09** | **98.14±0.07** | **99.48±0.05** |

To assess the consistency of the performance differences, paired Wilcoxon signed-rank tests were conducted over 10 matched runs between SGNet-IDS and FT-Transformer. SGNet-IDS outperformed FT-Transformer in all 10 runs for F1-score on both datasets. The mean paired improvements were 0.36 percentage points on CSE-CIC-IDS2018 and 0.28 percentage points on CIC-IoT-DIAD2024. The exact two-sided Wilcoxon signed-rank tests yielded W=0 and p=0.0019 for both datasets, indicating statistically significant

improvements at the 0.05 level. These results, together with the consistent improvement across all paired runs, support the stability of the observed F1-score gains.

Table 4 presents the class-wise performance of SGNet-IDS on the CIC-IoT-DIAD2024 dataset. The proposed framework achieved consistently high recall across all attack categories, exceeding 98.8%, indicating reliable detection of both common and infrequent attacks. The highest F1-score was obtained for DoS, with an F1-score of 0.9941, followed by distributed denial-of-service (DDoS), with an F1-score of 0.9892. reflecting the effectiveness of semantic group learning in modeling dominant traffic behaviors. Lower precision was observed for Web-Based and BruteForce attacks, primarily due to their limited number of test samples and behavioral similarity with other attack categories. Nevertheless, the high recall achieved for these minority classes demonstrates that SGNet-IDS preserves attack detection capability while maintaining strong overall multiclass performance.

Table 4. Per-class detection performance of SGNet-IDS on the CIC-IoT-DIAD2024 dataset

| Attack class | Test samples | Precision | Recall | F1-score |
|---|---|---|---|---|
| Web-Based | 2,266 | 0.8037 | 0.9881 | 0.8864 |
| Spoofing | 31,448 | 0.9276 | 0.9897 | 0.9577 |
| Recon | 88,432 | 0.9543 | 0.9886 | 0.9712 |
| Mirai | 34,918 | 0.8512 | 0.9896 | 0.9152 |
| DoS | 1,579,775 | 0.9982 | 0.9900 | 0.9941 |
| DDoS | 694,763 | 0.9883 | 0.9900 | 0.9892 |
| BruteForce | 724 | 0.7068 | 0.9890 | 0.8244 |

Table 5 presents the ablation study conducted to evaluate the contribution of the individual components of SGNet-IDS. Removing semantic grouping resulted in the largest performance degradation, indicating that behavior-oriented feature organization provides an important foundation for the proposed framework. Excluding the SGIM further reduced accuracy and F1-score, demonstrating the contribution of modeling interactions among semantic feature groups. Replacing adaptive weighting with uniform semantic aggregation also decreased performance, indicating that learnable feature weighting enhances the discriminative capability of the latent behavioral representation. The results indicate that each component contributes to the final performance, with the complete SGNet-IDS framework achieving the best results.

Table 5. Ablation analysis of the proposed SGNet-IDS framework

| Configuration | Accuracy (%) | F1-score (%) |
|---|---|---|
| Without semantic grouping | 98.95±0.18 | 97.93±0.22 |
| Without SGIM | 99.34±0.15 | 98.54±0.19 |
| Random feature grouping | 99.42±0.24 | 98.74±0.31 |
| Uniform semantic aggregation | 99.51±0.11 | 98.81±0.14 |
| SGNet-IDS (proposed) | 99.71±0.05 | 99.14±0.07 |

To examine whether the performance gain results from semantic organization rather than merely from feature partitioning, a random feature grouping configuration was evaluated using the same number and size of groups while keeping the remaining model components unchanged. As shown in Table 5, random grouping achieved 99.42% accuracy and 98.74% F1-score, whereas the proposed semantic grouping achieved 99.71% and 99.14%, respectively. The corresponding improvements of 0.29 and 0.40 percentage points indicate that the behavioral organization of features contributes beyond grouping alone. These results support the role of the domain-guided semantic structure in constructing more discriminative representations.

Table 6 compares the computational complexity and inference efficiency of SGNet-IDS with representative intrusion detection models under central processing unit (CPU) and graphics processing unit (GPU) execution. Latency was measured on an Intel Core i7-12700 CPU (single-thread mode) and an NVIDIA RTX 3080 GPU, using the average inference latency per sample over 1,000 iterations after a 100-sample warm-up. Although SGNet-IDS incorporates semantic interaction learning, its computational overhead remains limited because interactions are computed over only five semantic groups rather than across the entire high-dimensional feature space. On CPU execution, SGNet-IDS achieves an inference latency of 8.1 ms per sample, compared with 14.1 ms for CNN-LSTM, while GPU execution reduces its latency to 1.1 ms per sample. Combined with 0.59 M parameters and 103 MB memory usage, these results support the potential deployment of SGNet-IDS in both resource-constrained edge gateways and centralized enterprise IDS environments.

Table 6. Computational complexity comparison of SGNet-IDS and representative intrusion detection methods

| Model | Parameters | CPU latency (ms/sample) | GPU latency (ms/sample) | Memory (MB) |
|---|---|---|---|---|
| CNN-LSTM | 1.32 M | 14.1 | 2.4 | 191 |
| MFE-ELM | 0.37 M | 6.8 | 1.4 | 79 |
| SGNet-IDS | 0.59 M | 8.1 | 1.1 | 103 |

Figure 2 shows the training and validation loss curves of SGNet-IDS. Both losses decreased steadily and converged after approximately 35 epochs, with only a small gap between the curves. This consistent convergence indicates stable optimization with no evident overfitting during training.

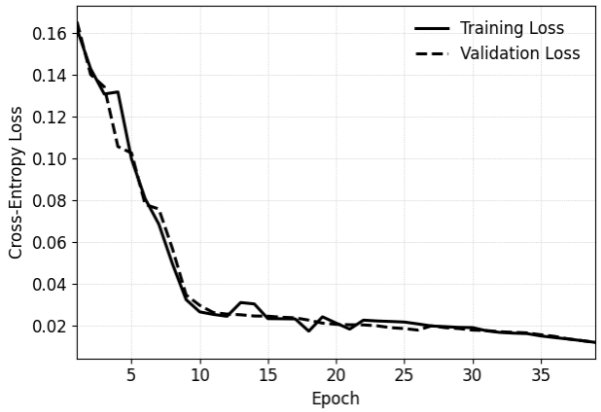



Figure 2. Training and validation convergence of SGNet-IDS

Figure 3 presents the normalized confusion matrix of SGNet-IDS on the CIC-IoT-DIAD2024 dataset. The diagonal values exceed 98.8% for all attack categories, while the largest confusion occurs between behaviorally similar DoS and Spoofing attacks. The remaining off-diagonal errors are below 0.5%, indicating strong multiclass discrimination despite class imbalance.

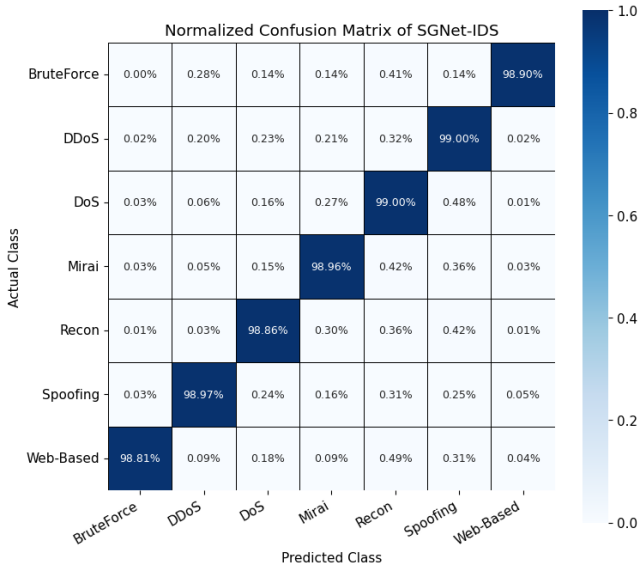



Figure 3. Normalized confusion matrix of SGNet-IDS on the CIC-IoT-DIAD2024 dataset

Figure 4 presents the ROC curves of SGNet-IDS on the CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 datasets. The corresponding AUC values are 0.987 and 0.973, respectively, with both curves remaining close

to the upper-left corner. These results indicate strong discrimination between benign and malicious traffic across both environments.

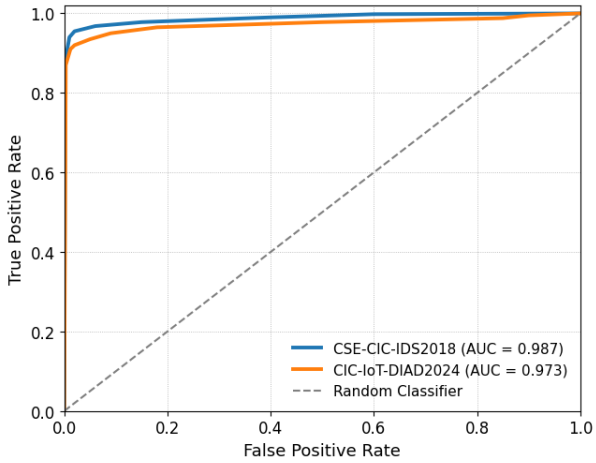



Figure 4. ROC curves of SGNet-IDS on the CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 datasets

The experimental results demonstrate that SGNet-IDS provides an effective framework for intrusion detection across enterprise and IoT network environments. By organizing network attributes into semantic behavioral groups and learning their interactions, SGNet-IDS captures complementary communication patterns that are not explicitly represented by individual flow features. This representation contributed to consistently high detection performance across both datasets while maintaining recall above 98.8% for all attack categories. The reduced precision observed for minority attack classes mainly reflects the severe class imbalance and behavioral overlap within the CIC-IoT-DIAD2024 dataset rather than a limitation of the proposed framework. Furthermore, the ablation study confirmed that semantic grouping, interaction learning, and adaptive feature weighting each contributed to the overall performance while maintaining moderate computational complexity.

## 4. CONCLUSION

This paper presented SGNet-IDS, a semantic group network learning framework for intrusion detection across enterprise and IoT network environments. By organizing normalized flow attributes into semantic behavioral groups and modeling their interactions through the SGIM, the proposed framework learns compact behavioral representations that improve intrusion classification without increasing classifier complexity. Experimental evaluation on the CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 datasets demonstrated that SGNet-IDS consistently achieved high detection accuracy and micro-averaged F1-score while maintaining competitive computational efficiency. Comparative evaluation against representative intrusion detection methods and stronger tabular learning baselines showed that the proposed semantic representation strategy achieved superior performance on both datasets. The ablation study further supported the individual contributions of semantic grouping, interaction learning, and adaptive feature weighting to the overall detection performance. These findings indicate that learning interactions among semantic behavioral groups provides an effective and computationally efficient approach to feature representation for intrusion detection. Future work will investigate adaptive semantic group construction and continual learning strategies to improve robustness under evolving attack patterns, concept drift, and emerging network protocols. A current limitation is that direct cross-dataset generalization was not explicitly evaluated, as CSE-CIC-IDS2018 and CIC-IoT-DIAD2024 exhibit differences in feature distributions and traffic characteristics. Evaluating the transferability of the learned semantic representations across heterogeneous network environments would provide further evidence of their generalization capability.

## FUNDING INFORMATION

Authors state no funding involved.

## AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sivakumaran Arumugam | ✓ | | ✓ | ✓ | ✓ | | | ✓ | ✓ | | | | ✓ | |
| Sumithra Mani | | ✓ | | | | ✓ | | ✓ | ✓ | | ✓ | ✓ | | |
| Anbarasu Rajabather | ✓ | | ✓ | ✓ | ✓ | | ✓ | | | ✓ | | | | |
| Rajesh Elangovan | | ✓ | | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | ✓ | |
| Arshita Srivastava | ✓ | | ✓ | | ✓ | | ✓ | | | ✓ | | ✓ | | |
| Prabhakaran Rajkumar | | ✓ | | ✓ | | ✓ | | ✓ | ✓ | | | | | |

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [initials: R.E], upon reasonable request.

## REFERENCES


[1] S. Chen and X. Fang, "Enhancing security in IoT-fog environments with a hybrid deep learning intrusion detection system," *Cluster Computing*, vol. 28, no. 15, Dec. 2025, doi: 10.1007/s10586-025-05714-1.

[2] W. M. Elsayed and A. A. Abohany, "Strengthening network resilience and optimizing resources in large enterprises: Innovative infrastructure and cybersecurity strategies," *Cluster Computing*, vol. 29, no. 4, May 2026, doi: 10.1007/s10586-026-06075-z.

[3] S. A. Abdulkareem, C. H. Foh, M. Shojafar, F. Carrez, and K. Moessner, "Network intrusion detection: An IoT and non IoT-related survey," *IEEE Access*, vol. 12, pp. 147167–147191, 2024, doi: 10.1109/ACCESS.2024.3473289.

[4] V. A. Memos, C. L. Stergiou, A. I. Bermperis, A. P. Plageras, and K. E. Psannis, "A novel architecture for mitigating botnet threats in AI-powered IoT environments," *Sensors*, vol. 26, no. 2, Jan. 2026, doi: 10.3390/s26020572.

[5] T. Al-Shurbaji *et al.*, "Deep learning-based intrusion detection system for detecting IoT botnet attacks: A review," *IEEE Access*, vol. 13, pp. 11792–11822, 2025, doi: 10.1109/ACCESS.2025.3526711.

[6] M. A. Issa, A. Eldosouky, A. Matrawy, and M. Ibnkahla, "Multi-temporal device clustering for federated learning-Internet of Things intrusion detection systems," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 4, pp. 1076–1102, 2026, doi: 10.1109/TMLCN.2026.3706262.

[7] S. Dardouri, "A deep learning approach using optimized LSTM for anomaly-based network intrusion detection," *Journal of Engineering*, no. 1, Jan. 2026, doi: 10.1155/je/2021709.

[8] J. Manoranjini, V. Gaddam, K. V. Raghavender, H. R. Battu, P. Sunitha, and S. K. Shanmugam, "Hybrid deep learning ensemble with score-based feature optimization for cyber attack detection in IoT systems," *Bulletin of Electrical Engineering and Informatics*, vol. 15, no. 3, pp. 2527–2536, Jun. 2026, doi: 10.11591/eei.v15i3.11674.

[9] A. Elayan and M. Kadoch, "Enhancing IoT network security: A BPSO-optimized attention-GRU deep learning framework for intrusion detection," *Computers*, vol. 15, no. 5, Apr. 2026, doi: 10.3390/computers15050266.

[10] R. Ponnumani, N. Vasudeva, T. Elumalai, P. Kaliyaperumal, B. Balusamy, and F. Benedetto, "A multi-stage framework for scalable and context-aware intrusion detection in IoT-cloud systems using deep latent modeling and graph-based attack classification," *Computers and Electrical Engineering*, vol. 131, Mar. 2026, doi: 10.1016/j.compeleceng.2026.110949.

[11] F. Ebrahimi, R. Javidan, R. Akbari, and Y. Hosseini, "Intrusion detection in the internet of things using convolutional neural networks: an explainable AI approach," *Cybersecurity*, vol. 8, p. 66, Sep. 2025, doi: 10.1186/s42400-025-00369-2.

[12] F. Chishti and G. Rathee, "An autonomous intrusion detection framework leveraging multi-layered stacking ensemble architectures with dynamic machine learning-driven feature subset optimisation," *Peer-to-Peer Networking and Applications*, vol. 19, no. 1, Jan. 2026, doi: 10.1007/s12083-025-02172-9.

[13] N. Dharini, V. S. Janani, and J. Katiravan, "Efficient detection of intrusions in TON-IoT dataset using hybrid feature selection approach," *Scientific Reports*, vol. 16, no. 1, Feb. 2026, doi: 10.1038/s41598-026-37834-y.

[14] P. Kaliyaperumal, T. Karuppiah, R. Perumal, M. Thirumalaisamy, B. Balusamy, and F. Benedetto, "Enhancing cybersecurity in Agriculture 4.0: A high-performance hybrid deep learning-based framework for DDoS attack detection," *Computers and Electrical Engineering*, vol. 126, Aug. 2025, doi: 10.1016/j.compeleceng.2025.110431.

[15] S. K. S *et al.*, "An unsupervised cloud-centric intrusion diagnosis framework using autoencoder and density-based learning," *Future Internet*, vol. 18, no. 1, Jan. 2026, doi: 10.3390/fi18010054.

[16] A. E. M. M L, P. S, M. Thirumalaisamy, P. Kaliyaperumal, B. Balusamy, and F. Benedetto, "A novel hybrid TabTransformer–LightGBM framework for explainable intrusion detection in smart farming IoT networks," *Computers and Electrical Engineering*,

vol. 138, Oct. 2026, doi: 10.1016/j.compeleceng.2026.111344.
[17] S. Alkadi, S. Al-Ahmadi, and M. M. B. Ismail, "Toward improved machine learning-based intrusion detection for Internet of Things traffic," *Computers*, vol. 12, no. 8, Jul. 2023, doi: 10.3390/computers12080148.
[18] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," *Computers*, vol. 12, no. 2, Feb. 2023, doi: 10.3390/computers12020034.
[19] V. Hnamte and J. Hussain, "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system," *Telematics and Informatics Reports*, vol. 10, Jun. 2023, doi: 10.1016/j.teler.2023.100053.
[20] M. Cantone, C. Marrocco, and A. Bria, "Machine learning in network intrusion detection: A cross-dataset generalization study," *IEEE Access*, vol. 12, pp. 144489–144508, 2024, doi: 10.1109/ACCESS.2024.3472907.
[21] V. M. de Oliveira, H. M. de Oliveira, G. M. Santos, J. Geremias, and E. K. Viegas, "A big data framework for scalable and cross-dataset capable machine learning in network intrusion detection systems," *IEEE Access*, vol. 13, pp. 129419–129431, 2025, doi: 10.1109/ACCESS.2025.3589872.
[22] M. Wang, N. Yang, Y. Guo, and N. Weng, "Learn-IDS: Bridging gaps between datasets and learning-based network intrusion detection," *Electronics*, vol. 13, no. 6, Mar. 2024, doi: 10.3390/electronics13061072.
[23] A. Raza, A. K. S. Ali, and A. A. Hussain, "AI-driven approaches to cyber and information security: Machine learning algorithms for threat prediction and anomaly detection," *Spectrum of Engineering Sciences*, vol. 2, no. 4, pp. 565–573, 2024.
[24] H. Lin, Q. Xue, J. Feng, and D. Bai, "Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine," *Digital Communications and Networks*, vol. 9, no. 1, pp. 111–124, Feb. 2023, doi: 10.1016/j.dcan.2022.09.021.
[25] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced intrusion detection systems performance with UNSW-NB15 data analysis," *Algorithms*, vol. 17, no. 2, Feb. 2024, doi: 10.3390/a17020064.
[26] M. A. Shyaa, N. F. Ibrahim, Z. B. Zainol, R. Abdullah, and M. Anbar, "Reinforcement learning-based voting for feature drift-aware intrusion detection: An incremental learning framework," *IEEE Access*, vol. 13, pp. 37872–37903, 2025, doi: 10.1109/ACCESS.2025.3544221.
[27] S. Yang, X. Zheng, J. Li, J. Xu, X. Wang, and E. C. H. Ngai, "ReCDA: Concept drift adaptation with representation enhancement for network intrusion detection," in *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, Aug. 2024, pp. 3818–3828, doi: 10.1145/3637528.3672007.
[28] R. Chu, P. Jin, H. Qiao, and Q. Feng, "Intrusion detection in the IoT data streams using concept drift localization," *AIMS Mathematics*, vol. 9, no. 1, pp. 1535–1561, 2023, doi: 10.3934/math.2024076.
[29] M. S. Noori, R. K. Z. Sahbudin, A. Sali, and F. Hashim, "Feature drift aware for intrusion detection system using developed variable length particle swarm optimization in data stream," *IEEE Access*, vol. 11, pp. 128596–128617, 2023, doi: 10.1109/ACCESS.2023.3333000.
[30] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116, doi: 10.5220/0006639801080116.
[31] M. Rabbani *et al.*, "Device identification and anomaly detection in IoT environments," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 13625–13643, May 2025, doi: 10.1109/JIOT.2024.3522863.

## BIOGRAPHIES OF AUTHORS



**Dr. Sivakumaran Arumugam** received his Ph.D. from Anna University, Chennai, in 2019, and his M.Tech. in Computer Science and Engineering from Motilal Nehru National Institute of Technology (NIT), Allahabad, in 2007. He has over 23 years of academic and research experience and is currently associated with RMK College of Engineering and Technology, Chennai. His research interests include web mining, deep learning, and machine learning. He has authored a Java programming book, published numerous research papers, holds five patents, and actively organizes workshops and serves as a session chair at international conferences. He can be contacted at email: sivakumaranads@rmkcet.ac.in.



**Dr. Sumithra Mani** is a professor in the Department of Information Technology at Panimalar Engineering College. With 20 years of teaching experience, she holds a Ph.D. and has authored 4 patents, 3 book chapters, and has published 15 research papers in renowned international journals and 30 papers in international conferences. Her areas of expertise include image processing, data mining applications, and machine learning. She can be contacted at email: msumithra@panimalar.ac.in.



**Anbarasu Rajabather** is an assistant professor at Manav Rachna International Institute of Research and Studies, India. He has over 18 years of professional experience, including 16 years in academia and two years in the software industry. He received his M.Tech. degree from Dr.M.G.R. Educational and Research Institute and he is currently pursuing a Ph.D. at Saveetha Institute of Medical and Technical Sciences. His research interests include computer science and emerging intelligent computing technologies. He can be contacted at email: anbu1812@gmail.com.



**Dr. Rajesh Elangovan** is a professor at the Alliance School of Advanced Computing, Alliance University, Bengaluru. He received his Ph.D. in Computer Science and Engineering from Anna University and has over 17 years of academic experience. His research interests include computational intelligence, soft computing, data science, IoT, and artificial intelligence (AI). He has published extensively in reputed journals and conferences, holds several patents, and is a member of IEEE and Association for Computing Machinery (ACM). He can be contacted at email: rajesh.e@alliance.edu.in.



**Arshita Srivastav** is an assistant professor in the Department of Computer Science and Applications (CSA), Sharda University, Uttar Pradesh. She received her M.Tech. in Computer Science and Engineering from Dr. A.P.J. Abdul Kalam Technical University (AKTU). With two years of teaching experience, her research interests include AI, ML, data science, and software engineering. She has participated in faculty development programs on scientometrics and generative AI and has served as a mentor for the Smart India Hackathon. She can be contacted at email: arshita.srivastava@sharda.ac.in.



**Prabhakaran Rajkumar** is an assistant professor in the Faculty of Computer Science and Information Technology at Vel Tech Multi Tech Engineering College. He received his bachelor's degree in Information Technology and master's degree in Computer Science and Engineering from Anna University. With over seven years of teaching experience in schools and higher education, his research interests include machine learning, deep learning, data analytics, wireless technologies, robotics, computational intelligence, virtual reality, and AI. He can be contacted at email: prabhakaran9495@gmail.com.