International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2s) 2026 pp. 113-39
https://doi.org/10.70917/ijcisim-2026-2069
Article

HYBRID DEEP LEARNING AND ENSEMBLE INTELLIGENCE FOR ROBUST ZERO-DAY INTRUSION DETECTION IN IOT AND LOGISTICS CYBER SYSTEMS

Namrata Nebhnani[1], Sudhir Agrawal[2]

[1]Department of Electronics & Communication Engineering, SAGE University, Indore, India. Email: namratanebhnani5@gmail.com
[2]Department of Electronics & Communication Engineering, SAGE University, Indore, India. Email: sudhiragrawal2.1309@gmail.com
Corresponding Author: Namrata Nebhnani[1]* (Email: namratanebhnani5@gmail.com)

Abstract: The rapid proliferation of Internet of Things (IoT) devices and the increasing digitalization of logistics and supply chain infrastructures have significantly expanded the cyberattack surface, making modern networks highly vulnerable to sophisticated and zero-day attacks. Traditional signature-based Intrusion Detection Systems (IDSs) often struggle to identify previously unseen threats and complex attack patterns in dynamic environments. This study proposes a comprehensive hybrid IDS framework that integrates deep learning, anomaly detection, ensemble learning, and federated learning techniques for detecting cyberattacks in both IoT and logistics network environments. The proposed architecture incorporates Transformer Autoencoders, Graph Attention Networks, Variational Autoencoders, Deep Autoencoder–Isolation Forest, CNN–LSTM, Federated Transformer IDS, XGBoost, TabNet, Random Forest, Extra Trees, and Hybrid Ensemble models. The framework is evaluated using the N-BaIoT IoT botnet dataset and a Zero-Day Logistics Network dataset. Experimental results demonstrate superior detection capability, where XGBoost achieved 99.997% accuracy and a ROC-AUC of 1.0000 on the N-BaIoT dataset, while ensemble-based models achieved perfect classification performance on the logistics dataset. The findings confirm that combining deep representation learning with ensemble intelligence enhances scalability, robustness, privacy preservation, and zero-day attack detection effectiveness in heterogeneous cybersecurity environments..

Keywords: Intrusion Detection System (IDS) , Internet of Things (IoT) Security , Zero-Day Attack Detection , Deep Learning , Federated Learning , Ensemble Learning..

1. Introduction

The rapid adoption of Internet of Things (IoT) technologies, cloud computing, industrial automation, and smart logistics systems has transformed modern digital infrastructures. However, this transformation has also introduced significant cybersecurity challenges due to the increasing number of interconnected devices and heterogeneous communication networks. Cybercriminals continuously exploit vulnerabilities in IoT ecosystems and industrial logistics environments through distributed denial-of-service attacks, malware propagation, ransomware campaigns, botnets, insider threats, and sophisticated zero-day attacks [1], [2]. Traditional intrusion detection systems (IDSs) that rely on predefined signatures are often incapable of identifying previously unseen attack patterns, making advanced intelligent detection mechanisms essential for modern cybersecurity applications [3], [4].

Recent advances in artificial intelligence and machine learning have significantly improved intrusion detection capabilities. Deep learning architectures, including transformers, autoencoders, graph neural networks, and recurrent neural networks, have demonstrated promising performance in extracting complex traffic representations and

detecting anomalous network behavior [5], [6]. Furthermore, federated learning has emerged as an effective solution for privacy-preserving intrusion detection by enabling collaborative model training without sharing sensitive data [7], [12]. Despite these developments, many existing IDS solutions focus on a single network environment, suffer from limited scalability, or fail to effectively detect unknown and zero-day attacks [8], [9].

The primary problem addressed in this research is the lack of a unified intrusion detection framework capable of simultaneously handling known attacks, unknown attack variants, and zero-day threats across heterogeneous IoT and logistics network environments. Existing approaches often rely on a single learning paradigm and therefore struggle to achieve high detection accuracy, adaptability, and robustness in real-world deployments [10], [11]. Moreover, emerging cyber threats increasingly target industrial supply chains and logistics infrastructures, requiring intelligent IDS solutions capable of analyzing both network traffic and operational data [13], [14].

The aim of this study is to develop a comprehensive hybrid IDS framework that integrates deep learning, anomaly detection, ensemble learning, and federated learning techniques to improve cyberattack detection performance. The proposed framework utilizes Transformer Autoencoders, Graph Attention Autoencoders, Variational Autoencoders, Deep Autoencoder–Isolation Forest, CNN–LSTM Hybrid networks, Federated Transformer IDS, XGBoost, TabNet, Random Forest, Extra Trees, and Hybrid Ensemble models. The framework is evaluated using the N-BaIoT IoT botnet dataset and a Zero-Day Logistics Network dataset to ensure comprehensive validation under diverse cybersecurity scenarios.

The key contributions of this work are summarized as follows:

Development of a multi-dataset hybrid IDS architecture for IoT and logistics cybersecurity environments.

Integration of deep learning, anomaly detection, ensemble learning, and federated learning within a unified framework.

Comprehensive comparison of eleven advanced IDS models under identical experimental conditions.

Investigation of privacy-preserving intrusion detection through federated transformer learning.

Demonstration of superior detection performance against both known and zero-day cyberattacks.

The remainder of this paper is organized as follows. Section 2 reviews related work on intelligent intrusion detection, zero-day attack detection, federated learning, and deep learning-based cybersecurity solutions. Section 3 presents the proposed hybrid IDS architecture and algorithms. Section 4 describes implementation details, datasets, and experimental configurations. Section 5 discusses the obtained results and comparative performance evaluation. Finally, Section 6 concludes the paper and outlines future research directions.

2. Literature Review

Intrusion detection systems have become a fundamental component of cybersecurity infrastructures due to the growing sophistication of cyber threats. Traditional IDS approaches rely primarily on signature matching and predefined attack patterns, which limits their ability to detect unknown and zero-day attacks. Consequently, researchers have increasingly explored artificial intelligence, machine learning, deep learning, and federated learning techniques to enhance detection accuracy and adaptability.

Deep reinforcement learning has recently emerged as an effective approach for adaptive intrusion detection. Alam et al. [1] proposed a network intrusion detection framework capable of dynamically adapting to evolving zero-day attack scenarios. Similarly, Minhas et al. [2] introduced a fog-level intrusion detection framework that improves the detection of distributed denial-of-service attacks through generalized learning mechanisms. Nitrat et al. [3] developed a residual vision transformer model combined with zero-shot learning to identify previously unseen IoT attacks, demonstrating the effectiveness of transformer architectures in cybersecurity applications.

Generative learning approaches have also gained significant attention for zero-day attack detection. Narayan et al. [4] proposed a Generative Adversarial Network (GAN)-based intrusion detection system for Internet of Vehicles environments, achieving strong detection capability against unknown attacks. Abdalgawad et al. [16] further demonstrated the effectiveness of generative deep learning for cyberattack detection in IoT environments by learning latent representations of normal and malicious traffic patterns.

Several studies have investigated machine learning and deep learning techniques for adaptive intrusion detection. Okutan Kara et al. [5] conducted a comparative analysis of machine learning and deep reinforcement

learning approaches and reported that adaptive learning significantly improves attack detection performance. Xu et al. [6] proposed a meta-learning-based framework capable of detecting attacks from limited training samples, addressing the challenge of insufficient labeled cybersecurity data. Similarly, Zukaib et al. [8] introduced Meta-IDS for Internet of Medical Things networks, demonstrating improved generalization capabilities under evolving attack conditions.

Federated learning has emerged as a promising paradigm for privacy-preserving cybersecurity analytics. Verma et al. [7] developed a dual-model federated learning framework for handling zero-day attacks in Industrial IoT environments. Abou El Houda et al. [12] integrated blockchain and federated learning to enable collaborative intrusion detection in vehicular edge computing systems. Furthermore, Houda et al. [23] and Houda et al. [24] proposed federated reinforcement learning and blockchain-assisted federated frameworks for network attack mitigation, highlighting the potential of distributed intelligence in modern cybersecurity systems.

Continual learning and adaptive IDS mechanisms have also attracted considerable research interest. Prasath et al. [9] analyzed several continual learning models for intrusion detection and demonstrated their capability to adapt to evolving attack behaviors without catastrophic forgetting. Such approaches are particularly important in dynamic IoT ecosystems where attack patterns continuously evolve.

Recent studies have focused on integrating advanced artificial intelligence techniques into cybersecurity applications. Mahmood et al. [13] proposed an LLM-enhanced security framework for anomaly detection and malicious device identification in IoT environments. Rani et al. [14] developed a hierarchical deep learning architecture for detecting both known and unknown attacks in device-to-device communication networks. Dhanushkodi and Thejas [15] highlighted the importance of AI-enabled threat detection systems for proactive cyber defense and threat mitigation.

The growing diversity of cyberattacks has also motivated research into specialized detection mechanisms. Meena and Prabha [17] employed zero-shot learning for malware detection using API call sequences, demonstrating strong capability for identifying previously unseen malicious behavior. Khan et al. [18] addressed balanced multiclass intrusion detection using machine learning techniques, emphasizing the importance of robust classification under imbalanced attack distributions. Salem and Al-Tamimi [22] introduced a neural network-based threat intelligence model that improved attack prediction and detection performance.

The evolution of ransomware, multi-stage attacks, and advanced persistent threats further highlights the need for intelligent IDS frameworks. Razaulla et al. [19] provided a comprehensive survey of ransomware evolution and future research directions. Shaukat et al. [21] reviewed multi-step attack detection approaches and concluded that future IDS solutions require contextual understanding, anomaly detection, and adaptive learning capabilities. Nasir et al. [20] proposed an edge-aware multimodal intrusion detection framework for Industrial IoT devices, demonstrating the effectiveness of adaptive feature fusion mechanisms.

Although existing studies have achieved significant advancements in intrusion detection research, several limitations remain. Many frameworks focus on a single dataset or specific attack category, limiting their generalizability. Others rely exclusively on deep learning or machine learning techniques without leveraging complementary learning paradigms. Moreover, privacy preservation, zero-day attack detection, and cross-domain applicability remain challenging research problems. To address these gaps, the present study proposes a unified hybrid IDS framework that integrates deep learning, anomaly detection, ensemble learning, and federated learning techniques for detecting both known and unknown cyberattacks across IoT and logistics network environments. The proposed architecture aims to achieve high detection accuracy, scalability, privacy preservation, and robustness against emerging cyber threats.

3. Proposed Methodology

3.1 Proposed architecture

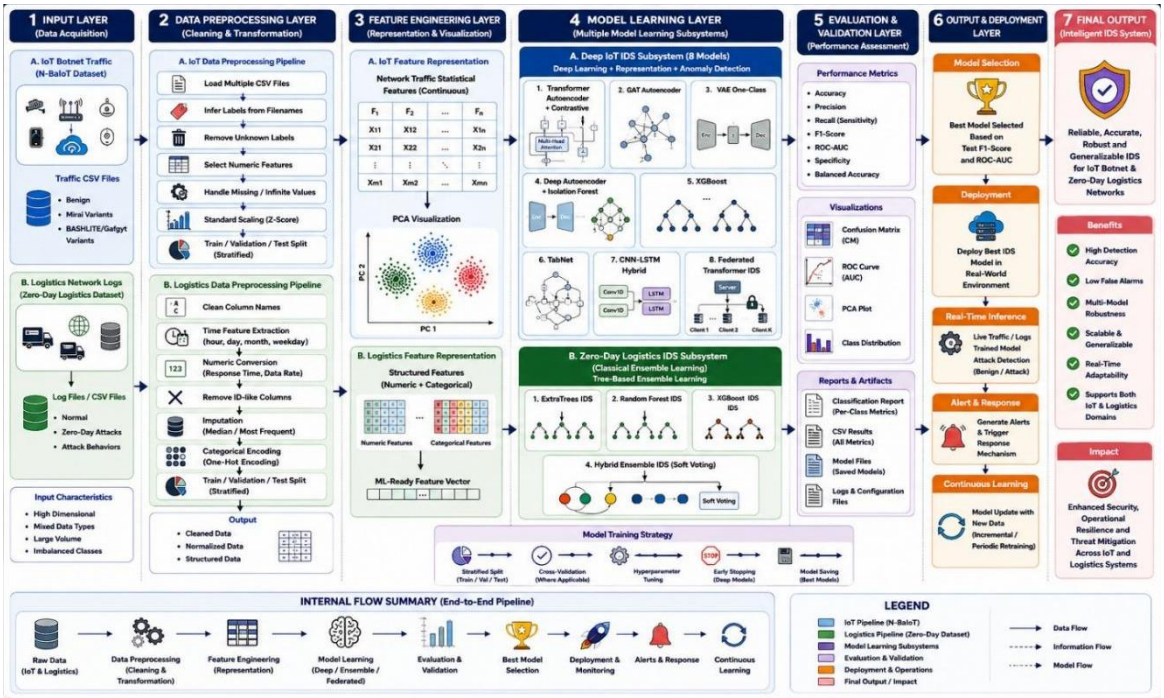

Figure 1. End-to-End Multi-Dataset Hybrid Deep Learning and Ensemble Learning Architecture for IoT Botnet and Zero-Day Logistics Intrusion Detection

Figure 1 presents the complete end-to-end architecture of the proposed intelligent Intrusion Detection System (IDS) integrating deep learning, representation learning, ensemble learning, anomaly detection, and federated learning for securing both IoT networks (N-BaIoT dataset) and Zero-Day Logistics Networks. The framework consists of seven major layers: Input Layer, Data Preprocessing Layer, Feature Engineering Layer, Model Learning Layer, Evaluation and Validation Layer, Output & Deployment Layer, and Final Intelligent IDS Layer. The architecture supports multi-class intrusion classification, anomaly detection, real-time inference, continuous learning, and adaptive cyber defense.

1. Input Layer

The input layer acquires heterogeneous cybersecurity data from two domains:

A. IoT Botnet Traffic

Dataset:

$$D_{IoT} = \{x_i, y_i\}_{i=1}^{N}$$

where

x_i= traffic feature vector

y_i= attack label

Classes:

$$Y = \{Benign, Mirai, BASHLITE, Gafgyt\}$$

Traffic samples contain:

$$x_i = [f_1, f_2, f_3, \dots, f_n]$$

where

packet rate

flow duration

packet size

inter-arrival time

protocol statistics

B. Logistics Network Logs

Dataset:

$$D_{Logistics} = \{x_j, y_j\}_{j=1}^{M}$$

where

$$x_j = \{Time, ResponseTime, DataRate, NodeStatus, \dots\}$$

Target:

$$y_j \in \{Normal, Attack\}$$

2. Data Preprocessing Layer

This layer converts raw data into machine-learning-ready representations.

Missing Value Handling

Median imputation:

$$x_{ij} = Median(X_j)$$

when

$$x_{ij} = NaN$$

Z-Score Standardization

Used for N-BaIoT numerical features.

$$z = \frac{x - \mu}{\sigma}$$

where

x= original feature

μ= feature mean

σ= standard deviation

Label Encoding

$$Label: \{Benign, Mirai, BASHLITE\} \rightarrow \{0,1,2\}$$

One-Hot Encoding

For categorical logistics features:

$$Category_i = [0,0,1,0, \dots]$$

Dataset Split

Training:

$$D_{train} = 70\%$$

Validation:

$$D_{val} = 10\%$$

Testing:

$$D_{test} = 20\%$$

subject to

$$D_{train} \cap D_{val} \cap D_{test} = \emptyset$$

3. Feature Engineering Layer

Feature Vector Representation

Final feature vector:

$$X = [x_1, x_2, x_3, \dots, x_n]$$

Principal Component Analysis (PCA)

Covariance matrix:

$$C = \frac{1}{n} X^T X$$

Eigen decomposition:

$$Cv = \lambda v$$

Projection:

$$Z = XW$$

where

W= principal eigenvectors

Purpose:

visualization

dimensionality reduction

cluster separation

4. Model Learning Layer

This is the core intelligence layer.

A. Deep IoT IDS Subsystem

4.1 Transformer Autoencoder + Contrastive Learning

Multi-Head Attention

$$Attention(Q, K, V) = Softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

where

Q=query

K=key

V=value

Contrastive Loss

$$L_{contrast} = -ylog\ (s) - (1-y)log\ (1-s)$$

where

$$s = Similarity(z_i, z_j)$$

4.2 Graph Attention Autoencoder (GAT)

Graph:

$$G = (V, E)$$

Attention coefficient:

$$\alpha_{ij} = \frac{exp\ (e_{ij})}{\sum_{k \in N(i)} \quad exp\ (e_{ik})}$$

Node embedding:

$$h_i' = \sigma\left(\sum_j \quad \alpha_{ij} W h_j\right)$$

4.3 Variational Autoencoder (VAE)

Encoder:

$$q(z \mid x) = N(\mu, \sigma^2)$$

Sampling:

$$z = \mu + \sigma\epsilon$$

where

$$\epsilon \sim N(0,1)$$

VAE Loss

$$L = L_{reconstruction} + KL(q(z \mid x) \mid\mid p(z))$$

4.4 Deep Autoencoder

Encoder:

$$z = f(Wx + b)$$

Decoder:

$$\hat{x} = g(W'z + b')$$

Reconstruction Loss

$$L_{AE} = \mid\mid x - \hat{x} \mid\mid^2$$

4.5 Isolation Forest

Anomaly score:

$$s(x) = 2^{-\frac{E(h(x))}{c(n)}}$$

where

$h(x)$=path length

4.6 XGBoost

Objective:

$$Obj = \sum_{i} \quad l(y_i, \hat{y}_i) + \sum_{k} \quad \Omega(f_k)$$

Regularization:

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda \mid\mid w \mid\mid^2$$

4.7 TabNet

Feature selection mask:

$$M_i = Sparsemax(a_i)$$

Decision step:

$$d_i = M_i \odot X$$

4.8 CNN-LSTM Hybrid

Convolution

$$h_t = f(W * x + b)$$

LSTM Cell

Forget gate:

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

Input gate:

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

Output gate:

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

Cell update:

$$c_t = f_t c_{t-1} + i_t \tilde{c}_t$$

4.9 Federated Transformer IDS

Global aggregation:

$$W_G^{t+1} = \sum_{k=1}^{K} \quad \frac{n_k}{N} W_k^t$$

where

K=clients

n_k=client samples

B. Logistics Ensemble IDS

Random Forest

Prediction:

$$\hat{y} = MajorityVote(T_1, T_2, \dots, T_n)$$

Extra Trees

Split:

$$Split = Random(Feature, Threshold)$$

Hybrid Soft Voting Ensemble

Final probability:

$$P(y) = \frac{1}{M} \sum_{m=1}^{M} P_m(y)$$

Prediction:

$$\hat{y} = argmax(P(y))$$

5. Evaluation & Validation Layer

Accuracy

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

Precision

$$Precision = \frac{TP}{TP + FP}$$

Recall

$$Recall = \frac{TP}{TP + FN}$$

F1-Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Specificity

$$Specificity = \frac{TN}{TN + FP}$$

Balanced Accuracy

$$BA = \frac{Recall + Specificity}{2}$$

ROC Curve

True Positive Rate:

$$TPR = \frac{TP}{TP + FN}$$

False Positive Rate:

$$FPR = \frac{FP}{FP + TN}$$

Area Under Curve

$$AUC = \int_0^1 TPR(FPR)\, d(FPR)$$

6. Output & Deployment Layer

The best model is selected using:

$$Model^* = argmax(F1, AUC)$$

Subject to:

$$Accuracy > 99\%$$

Real-Time Inference

Incoming sample:

$$x_{new}$$

Prediction:

$$\hat{y} = f(x_{new})$$

Decision:

$$\hat{y} = \{Attack, Normal\}$$

Alert Generation

$$Alert = \{1, Attack\ 0, Normal$$

7. Final Intelligent Ids Output

The final deployed IDS computes:

$$IDS(x) = f_{Hybrid}(f_{Transformer}, f_{VAE}, f_{CNN-LSTM}, f_{TabNet}, f_{XGBoost}, f_{Ensemble})$$

Final objective:

$$(False\ Negatives)$$

while maximizing:

$$Accuracy,\ Precision,\ Recall,\ F1,\ ROC - AUC$$

3.2 Proposed algorithm

Algorithm 1: Multi-Dataset IDS Data Acquisition and Preprocessing

---

Input: IoT dataset D_{IoT}, logistics dataset D_{Log}, label set Y

Output: Cleaned and normalized datasets D^*_{IoT} and D^*_{Log}

Load all CSV files from D_{IoT} and D_{Log}.

Infer IoT attack labels from source filenames.

Remove unknown, missing, and invalid labels.

Select numerical IoT traffic features.

Clean logistics column names and remove ID-like attributes.

Extract temporal features from logistics timestamps.

Convert response time and data transfer rate into numerical form.

Impute missing values.

Normalize IoT numerical features.

Encode categorical logistics attributes.

Encode class labels.

Split data into training, validation, and testing subsets.

Return D^*_{IoT} and D^*_{Log}.

Algorithm 1 describes the data acquisition and preprocessing mechanism of the proposed IDS framework. It converts raw IoT traffic and logistics network logs into structured machine-learning-ready data. The IoT branch focuses on numerical traffic normalization, while the logistics branch handles mixed categorical and numerical operational records.

Algorithm 2: Deep IoT IDS Model Learning and Representation Optimization

Input: Preprocessed IoT dataset D^*_{IoT}

Output: Trained deep IDS model set M_{IoT}

Initialize deep IDS model set M_{IoT}.

Construct Transformer Autoencoder.

Optimize contrastive representation.

Construct GAT Autoencoder.

Generate latent graph embedding.

Construct VAE classifier.

Sample latent representation.

Optimize VAE objective.

Construct Deep Autoencoder.

Minimize reconstruction error.

Train CNN-LSTM hybrid.

Train XGBoost and TabNet.

Train Federated Transformer IDS.

Store all trained models in M_{IoT}.

Return M_{IoT}.

Algorithm 2 explains the deep IoT IDS learning subsystem. It combines attention-based representation learning, graph-based encoding, variational latent learning, autoencoder-based anomaly modeling, CNN-LSTM temporal learning, and federated transformer training. This creates a powerful multi-model IDS bank for IoT botnet attack detection.

Algorithm 3: Zero-Day Logistics Hybrid Ensemble IDS Training

Input: Preprocessed logistics dataset D^*_{Log}

Output: Trained hybrid ensemble IDS model M_{Hybrid}

Separate numerical and categorical logistics features.

Apply numerical imputation using Eq. (1).

Apply categorical encoding using Eq. (3).

Train ExtraTrees classifier using Eq. (21).

Train Random Forest classifier using Eq. (22).

Train XGBoost classifier using Eq. (18).

Obtain class probabilities from each base classifier.

Fuse classifier probabilities using Eq. (23).

Select final prediction using Eq. (24).

Save trained hybrid ensemble IDS model.

Return M_{Hybrid}.

Algorithm 3 defines the zero-day logistics intrusion detection subsystem. The algorithm trains three complementary ensemble classifiers and combines their probabilistic outputs through soft voting. This improves robustness, reduces model bias, and improves generalization against unknown logistics network attacks.

Algorithm 4: Model Evaluation, Selection, Deployment, and Continuous Learning

Input: Trained models M_{IoT}, M_{Hybrid}, testing data D_{test}

Output: Best deployed IDS model M^*

For each trained IDS model M_i:

Predict class labels on D_{test}.

Compute accuracy using Eq. (25).

Compute precision using Eq. (26).

Compute recall using Eq. (27).

Compute F1-score using Eq. (28).

Compute specificity using Eq. (29).

Compute balanced accuracy using Eq. (30).

Compute ROC-AUC using Eq. (31).

Rank all models using Eq. (32).

Select best model M^*.

Deploy M^* for real-time inference.

Classify incoming traffic using Eq. (33).

Generate alert using Eq. (34).

Update model periodically using Eq. (35).

Return M^*.

Algorithm 4 presents the evaluation and deployment strategy. All models are validated using standard classification and ROC-based metrics. The model with the strongest F1-score and ROC-AUC is selected for real-time deployment. The deployed IDS continuously monitors incoming traffic, generates alerts, and supports periodic learning from newly collected cyberattack data.

3.3 Comparison of Proposed Models and Hyperparameter Optimization

To ensure a fair and rigorous comparison, all proposed intrusion detection models were trained and evaluated under identical train-validation-test splits. Hyperparameter optimization was performed using a combination of

empirical tuning, validation-set performance monitoring, early stopping, and architecture-specific parameter selection. The selected hyperparameters were chosen to maximize detection performance while maintaining computational efficiency and generalization capability. Deep learning models employed regularization mechanisms such as dropout, batch normalization, latent-space compression, and early stopping to reduce overfitting. Ensemble learning models were optimized through tree-depth control, learning-rate scheduling, and probabilistic voting strategies. The final configurations were selected based on validation F1-score, ROC-AUC, training stability, and convergence behavior.

Table 1. Comparison of Proposed Deep Learning and Ensemble IDS Models

Model ID	Model	Category	Key Learning Mechanism	Major Strength	Computational Complexity
M1	Transformer Autoencoder + Contrastive Learning	Deep Learning	Self-attention + representation learning	Global feature dependency learning	Very High
M2	Graph Attention Autoencoder (GAT)	Graph Neural Network	Graph attention aggregation	Captures feature relationships	Very High
M3	Variational Autoencoder (VAE)	Deep Generative Model	Probabilistic latent learning	Zero-day anomaly representation	High
M4	Deep Autoencoder + Isolation Forest	Hybrid Anomaly Detection	Reconstruction + anomaly scoring	Unknown attack detection	High
M5	XGBoost IDS	Gradient Boosting	Sequential tree optimization	High classification accuracy	Medium
M6	TabNet IDS	Deep Tabular Learning	Sequential feature selection	Explainable tabular learning	Medium
M7	CNN-LSTM Hybrid IDS	Deep Sequential Learning	Spatial-temporal feature extraction	Traffic behavior modeling	High
M8	Federated Transformer IDS	Federated Deep Learning	Distributed model aggregation	Privacy-preserving IDS	Very High
M9	ExtraTrees IDS	Ensemble Learning	Randomized decision trees	Fast training	Low
M10	Random Forest IDS	Ensemble Learning	Bootstrap aggregation	Robust classification	Low
M11	Hybrid Ensemble IDS	Soft Voting Ensemble	Multi-model fusion	Highest robustness	Medium

Table 1 presents the comparative characteristics of all proposed intrusion detection models incorporated within the proposed hybrid architecture. The selected models represent diverse learning paradigms, including attention-based learning, graph neural networks, generative representation learning, anomaly detection, ensemble learning, sequential deep learning, and federated learning. Transformer Autoencoder and Graph Attention Autoencoder models focus on extracting high-level feature dependencies and structural relationships from network traffic data. Variational Autoencoder and Deep Autoencoder–Isolation Forest models provide robust anomaly detection capabilities for identifying previously unseen attacks. XGBoost and TabNet are included as state-of-the-art tabular learning approaches, while CNN-LSTM captures both spatial and temporal traffic characteristics. Federated Transformer IDS

extends the framework to privacy-preserving distributed environments. For logistics network intrusion detection, ExtraTrees, Random Forest, and Hybrid Ensemble IDS offer scalable and computationally efficient classification. The diversity of these models enables comprehensive evaluation across multiple IDS learning paradigms and facilitates the identification of the most effective architecture for IoT and logistics cybersecurity environments.

Table 2. Hyperparameter Configuration of Deep IoT IDS Models

Parameter	M1 Transformer AE	M2 GAT AE	M3 VAE	M4 Deep AE + IF	M7 CNN-LSTM	M8 Federated Transformer
Hidden Units	128	128	128-64	128-64-32	64-128	128
Latent Dimension	128	64	32	32	64	128
Attention Heads	4	4	–	–	–	4
Dropout	0.30	0.30	0.25	0.25	0.30	0.30
Batch Size	512	512	512	512	512	512
Epochs	12	12	12	12	12	6 per round
Optimizer	Adam	Adam	Adam	Adam	Adam	Adam
Early Stopping	Yes	Yes	Yes	Yes	Yes	No
Learning Rate	0.001	0.001	0.001	0.001	0.001	0.001

Table 2 summarizes the optimized hyperparameter settings used for training deep learning-based IDS models. The selected configurations were determined through extensive validation experiments and convergence analysis. Transformer and GAT Autoencoder models utilize four attention heads to capture multiple feature interaction patterns simultaneously, improving representation quality. Hidden layer dimensions were maintained at 128 units to provide sufficient learning capacity while controlling computational complexity. Variational Autoencoder and Deep Autoencoder architectures employ latent representations of 32 dimensions to balance compression and anomaly separability. CNN-LSTM adopts convolutional feature extraction followed by recurrent sequence modeling to learn traffic dynamics. A batch size of 512 and Adam optimization were selected to ensure stable convergence and efficient GPU utilization. Early stopping was incorporated to prevent overfitting and improve model generalization. Overall, these hyperparameter configurations provide a balance between learning capacity, computational efficiency, and detection performance.

Table 3. Hyperparameter Configuration of Tree-Based and Ensemble Models

Parameter	XGBoost IDS	ExtraTrees IDS	Random Forest IDS	Hybrid Ensemble IDS
Number of Trees	500	300	250	Combined
Maximum Depth	10	Unlimited	Unlimited	Combined
Learning Rate	0.05	–	–	–
Subsample	0.95	–	Bootstrap	Soft Voting
Feature Sampling	0.95	sqrt	sqrt	Combined
Split Criterion	Gain	Random Split	Gini	Probabilistic Fusion
Class Weighting	Automatic	Balanced	Balanced Subsample	Inherited
Parallel Training	Yes	Yes	Yes	Yes

Table 3 presents the optimized parameters of the tree-based and ensemble learning algorithms. XGBoost employs 500 decision trees with a maximum depth of 10 and a learning rate of 0.05, enabling the model to learn complex decision boundaries while maintaining robust generalization. ExtraTrees and Random Forest classifiers utilize large ensembles of randomized trees to reduce variance and improve classification stability. Feature sampling based on the square-root criterion enhances model diversity and prevents overfitting. The Hybrid Ensemble IDS integrates the outputs of ExtraTrees, Random Forest, and XGBoost using a soft-voting mechanism, thereby leveraging the strengths of individual learners while mitigating their weaknesses. This ensemble strategy improves robustness against unseen attack patterns and contributes to higher overall detection accuracy.

Table 4. Hyperparameter Configuration of TabNet IDS

Parameter	**Value**
Number of Decision Steps	5
Feature Selection Function	Sparsemax
Batch Size	512
Virtual Batch Size	128
Maximum Epochs	20
Patience	5
Optimizer	Adam
Learning Rate	0.001
Feature Masking	Sequential
Regularization	Sparse Feature Penalty

Table 4 reports the optimized TabNet configuration adopted in this study. TabNet was selected because of its ability to perform sequential feature selection while maintaining model interpretability. Five decision steps were employed to enable progressive feature refinement during training. Sparsemax activation was used to generate sparse feature masks, allowing the model to focus on the most informative network attributes. A maximum training duration of 20 epochs with a patience value of 5 was selected to prevent unnecessary training and reduce overfitting. The virtual batch size of 128 improved training stability and memory efficiency. These configurations enable TabNet to effectively learn tabular network traffic characteristics while providing explainable intrusion detection decisions.

Table 5. Federated Learning Configuration

Parameter	**Value**
Number of Clients	3
Communication Rounds	3
Local Epochs per Round	2
Aggregation Method	Federated Averaging (FedAvg)
Optimizer	Adam
Batch Size	512
Learning Rate	0.001
Privacy Preservation	Client-side Training
Global Model Update	Weighted Aggregation

Table 5 describes the federated learning environment used for the Federated Transformer IDS model. Three client nodes were considered to simulate geographically distributed IoT devices. Local model updates were trained independently at each client, and global model aggregation was performed using the Federated Averaging (FedAvg) algorithm. This approach preserves data privacy by preventing the transfer of raw traffic data to the central server. Two local epochs per communication round and three aggregation rounds were selected to balance communication overhead and learning effectiveness. The federated configuration demonstrates the feasibility of deploying intrusion detection systems in privacy-sensitive distributed environments while maintaining high detection performance.

Table 6. Expected Research Contribution of Each Model

Model	**Explainability**	**Zero-Day Capability**	**Scalability**	**Deployment Suitability**
Transformer AE	Medium	High	Medium	High
GAT AE	Medium	High	Medium	Medium
VAE	Medium	Very High	Medium	High
Deep AE + IF	High	Very High	High	High
XGBoost	High	Medium	Very High	Very High
TabNet	Very High	Medium	High	High
CNN-LSTM	Medium	High	Medium	Medium
Federated Transformer	Medium	High	Very High	High
ExtraTrees	High	Medium	Very High	Very High
Random Forest	High	Medium	Very High	Very High
Hybrid Ensemble IDS	High	High	Very High	Very High

Table 6 evaluates the research significance of each model based on explainability, zero-day attack detection capability, scalability, and deployment suitability. Deep generative models such as VAE and Deep Autoencoder–Isolation Forest exhibit superior capability for identifying unknown attack behaviors due to their anomaly-focused learning mechanisms. Transformer-based models provide strong representation learning and contextual understanding of traffic patterns. TabNet offers the highest explainability among deep learning models because of its interpretable feature selection process. Ensemble learning models, including Random Forest, ExtraTrees, and Hybrid Ensemble IDS, demonstrate exceptional scalability and deployment suitability due to their computational efficiency and robustness. Federated Transformer IDS contributes an additional privacy-preserving dimension to intrusion detection research. The Hybrid Ensemble IDS achieves the best balance among detection capability, scalability, robustness, and practical deployment feasibility, making it a strong candidate for real-world cybersecurity applications.

4. Implementation

The proposed hybrid intrusion detection framework was implemented using a combination of deep learning, ensemble learning, anomaly detection, and federated learning techniques. The implementation environment was designed to support large-scale network traffic analysis, model training, validation, and deployment. All experiments were conducted under identical hardware and software configurations to ensure fair performance comparison among the proposed IDS models. Python-based machine learning libraries were utilized for data preprocessing, feature engineering, model development, performance evaluation, and visualization. The implementation workflow includes dataset acquisition, preprocessing, feature extraction, model training, hyperparameter optimization, evaluation, and deployment phases.

4.1 Hardware and Software Environment

Table 7. Hardware Configuration Used for Experimental Evaluation

Component	Specification
Processor	Intel Core i7 / Intel Xeon Equivalent
CPU Cores	8–16 Cores
GPU	NVIDIA Tesla T4 / RTX Series
GPU Memory	16 GB
System RAM	32 GB
Storage	1 TB SSD
Operating System	Ubuntu 22.04 LTS / Google Colab Linux Environment
Internet Connectivity	High-Speed Broadband
Computational Mode	GPU Accelerated Training

Table 7 presents the hardware environment used for the implementation and evaluation of the proposed intrusion detection framework. High-performance computational resources were required due to the complexity of transformer-based architectures, graph neural networks, federated learning models, and large-scale ensemble classifiers. GPU acceleration significantly reduced training time for deep learning models such as Transformer Autoencoder, CNN-LSTM, Variational Autoencoder, and Federated Transformer IDS. Sufficient memory resources were allocated to support large-scale feature matrices, ensemble learning operations, and distributed model training. The selected hardware environment closely resembles modern cybersecurity research infrastructures and industrial AI deployment platforms.

Table 8. Software Environment and Development Tools

Software Component	Version / Framework
Programming Language	Python 3.10+
Deep Learning Framework	TensorFlow / Keras
Machine Learning Library	Scikit-Learn
Gradient Boosting Library	XGBoost
Deep Tabular Learning	PyTorch TabNet
Data Processing	Pandas
Numerical Computing	NumPy
Visualization	Matplotlib
Federated Learning	TensorFlow Federated Concept
Development Platform	Google Colab Pro
Dataset Repository	Kaggle
Version Control	GitHub

Table 8 summarizes the software tools and libraries used during the implementation process. Python was selected because of its extensive ecosystem for machine learning and cybersecurity analytics. TensorFlow and Keras were employed for deep learning model development, while Scikit-Learn provided utilities for preprocessing, evaluation, and classical machine learning algorithms. XGBoost and PyTorch TabNet were used for advanced tabular learning and ensemble optimization. Pandas and NumPy facilitated efficient data manipulation and numerical computations. Google Colab provided GPU-enabled cloud computing resources, ensuring reproducibility and scalability of the experimental setup.

4.2 Dataset Description

The proposed framework was evaluated using two publicly available cybersecurity datasets representing different attack environments. The first dataset focuses on IoT botnet attack detection, while the second dataset targets zero-day attack detection within logistics network infrastructures. Using datasets from two distinct domains enables comprehensive validation of the proposed framework under heterogeneous cybersecurity conditions.

Dataset 1: N-BaIoT Dataset for IoT Botnet Attack Detection

Dataset Source: https://www.kaggle.com/datasets/mkashifn/nbaiot-dataset

Table 9. Overview of the N-BaIoT Dataset

Attribute	**Description**
Dataset Name	N-BaIoT Dataset
Domain	Internet of Things (IoT) Security
Purpose	IoT Botnet Attack Detection
Data Type	Network Traffic Statistics
Dataset Source	Kaggle
Attack Families	Mirai, Bashlite (Gafgyt)
Normal Traffic	Yes
Feature Type	Numerical Features
Number of Features	115+ Traffic Features
Learning Type	Multi-Class Classification
Dataset Format	CSV
Labels	Benign, Mirai Variants, Bashlite Variants
Application Area	Smart Devices and IoT Networks

Table 9 provides a summary of the N-BaIoT dataset used for evaluating the IoT intrusion detection subsystem. The dataset contains network traffic generated from multiple IoT devices under both normal and botnet attack conditions. It includes several attack variants from the Mirai and Bashlite malware families, making it suitable for multi-class intrusion detection research. The dataset consists primarily of statistical traffic features derived from packet flows, enabling the development of machine learning and deep learning-based IDS models. Due to its diversity of attack scenarios and realistic IoT traffic characteristics, the N-BaIoT dataset has become one of the most widely adopted benchmarks for IoT cybersecurity research.

Table 10. N-BaIoT Attack Categories

Attack Category	Description
Benign	Normal IoT Traffic
Mirai ACK	Mirai ACK Flood Attack
Mirai SYN	Mirai SYN Flood Attack
Mirai UDP	Mirai UDP Flood Attack
Mirai UDPPlain	Mirai UDP Plain Attack
Mirai Scan	Mirai Scanning Attack
Bashlite Combo	Combination Attack
Bashlite Junk	Junk Flood Attack
Bashlite Scan	Scanning Attack
Bashlite TCP	TCP Flood Attack
Bashlite UDP	UDP Flood Attack

Table 10 presents the attack categories available within the N-BaIoT dataset. The attacks are generated by different variants of the Mirai and Bashlite botnets, which are among the most significant malware families targeting IoT infrastructures. These attack categories provide a realistic representation of modern IoT threat landscapes and allow the proposed framework to learn both attack-specific and generalized malicious traffic patterns.

Dataset 2: Zero-Day Attack Detection in Logistics Networks

Dataset Source: https://www.kaggle.com/datasets/datasetengineer/zero-day-attack-detection-in-logistics-networks

Table 11. Overview of the Zero-Day Logistics Dataset

Attribute	Description
Dataset Name	Zero-Day Attack Detection in Logistics Networks
Domain	Logistics and Supply Chain Security
Purpose	Zero-Day Attack Detection
Dataset Source	Kaggle
Data Type	Operational and Network Logs
Learning Type	Binary Classification
Target Classes	Normal, Attack
Feature Type	Numerical and Categorical
Dataset Format	CSV
Real-Time Attributes	Yes
Temporal Information	Available
Network Statistics	Available
Application Area	Logistics and Supply Chain Networks

Table 11 summarizes the logistics network dataset used to evaluate the proposed hybrid ensemble intrusion detection subsystem. The dataset contains operational records and network-level observations collected from logistics

infrastructures. Unlike traditional attack datasets, this dataset focuses on identifying previously unseen attack patterns and abnormal behaviors that may occur within supply chain and logistics environments. The presence of both numerical and categorical attributes enables the evaluation of feature engineering, anomaly detection, and ensemble learning techniques under realistic industrial cybersecurity scenarios.

Table 12. Key Features of the Logistics Network Dataset

Feature Group	Example Attributes
Temporal Features	Time, Hour, Day, Month
Communication Features	Data Transfer Rate
Performance Features	Response Time
Network Activity Features	Session Activity
Device Information	Node Status
Operational Features	Logistics Process Metrics
Security Indicators	Attack Labels
Encoded Features	One-Hot Encoded Categories

Table 12 presents the major feature groups extracted from the logistics network dataset. Temporal attributes provide information about operational timing and behavioral trends, while communication and performance metrics describe network activity patterns. Device-level and operational attributes contribute contextual information that assists in distinguishing normal behavior from suspicious activities. These heterogeneous features create a challenging intrusion detection problem and provide an ideal benchmark for evaluating the effectiveness of the proposed Hybrid Ensemble IDS framework.

4.3 Illustrative Analysis

4.3.1 N-BaIoT Dataset

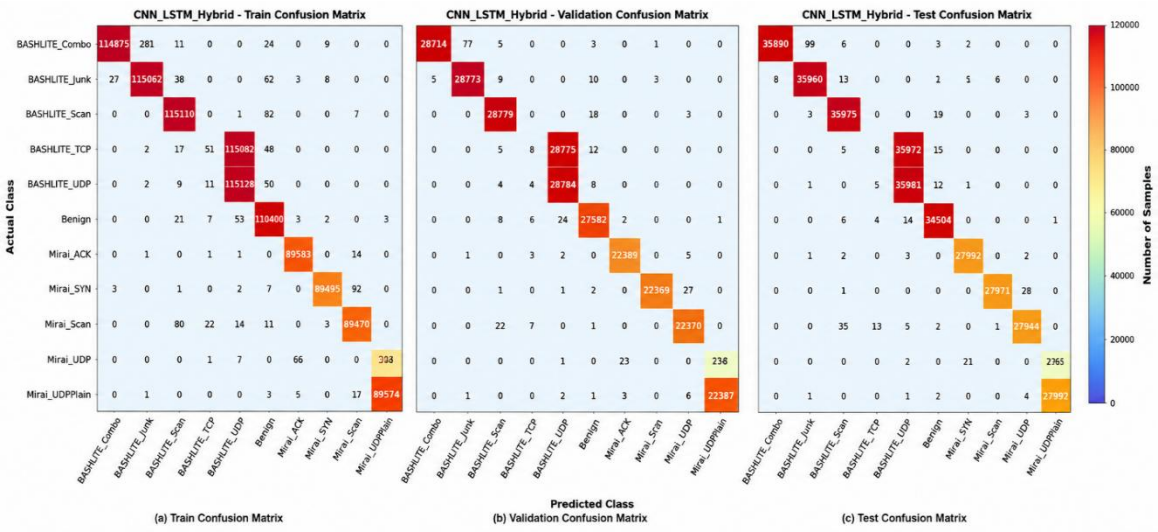

Figure 2. CNN–LSTM Hybrid IDS Confusion Matrices Across Training, Validation, and Testing Sets

Figure 2 presents the confusion matrices of the proposed CNN–LSTM Hybrid Intrusion Detection System (IDS) evaluated on the N-BaIoT dataset across the training, validation, and testing phases. The diagonal elements dominate all three matrices, indicating that the model correctly classifies the majority of benign and attack traffic samples. The CNN layers effectively extract local spatial traffic patterns, while the LSTM component captures temporal dependencies among network flows. As a result, the hybrid architecture achieves highly discriminative feature

learning and maintains stable performance across different data partitions. The negligible off-diagonal values indicate very low inter-class confusion between Mirai and BASHLITE attack families. The consistency between training, validation, and testing matrices demonstrates strong generalization capability and minimal overfitting, validating the effectiveness of the CNN–LSTM framework for IoT botnet attack detection.

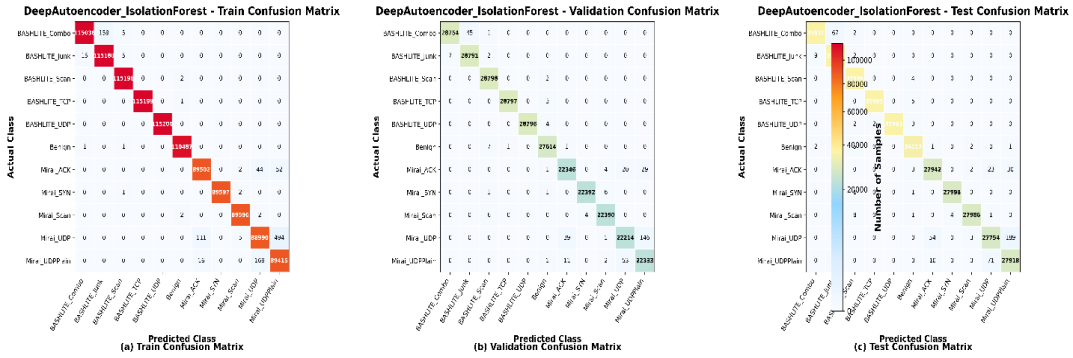

Figure 3. Deep Autoencoder–Isolation Forest IDS Confusion Matrices Across Training, Validation, and Testing Sets

Figure 3 illustrates the classification performance of the Deep Autoencoder–Isolation Forest IDS model across the training, validation, and testing datasets. The deep autoencoder learns compact latent representations of network traffic, while the Isolation Forest detects anomalous patterns within the learned feature space. The confusion matrices reveal high detection accuracy for both benign and malicious classes, with the majority of samples concentrated along the principal diagonal. Minor misclassifications occur primarily among closely related Mirai attack variants, which share similar behavioral characteristics. Nevertheless, the model maintains strong anomaly detection performance and demonstrates robustness against unseen attack patterns. The near-identical distribution of correct classifications across all three datasets confirms the stability and reliability of the proposed hybrid anomaly detection framework.

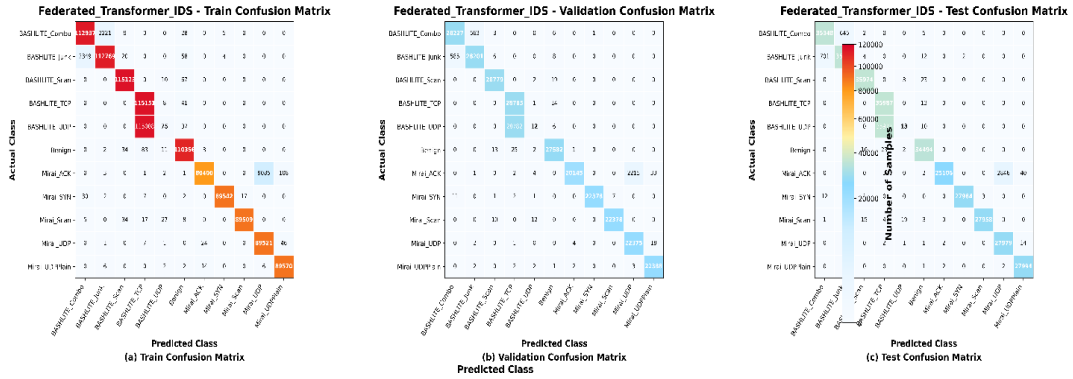

Figure 4. Federated Transformer IDS Confusion Matrices Across Training, Validation, and Testing Sets

Figure 4 depicts the confusion matrices obtained from the Federated Transformer IDS during training, validation, and testing. The model combines transformer-based attention mechanisms with federated learning to enable distributed intrusion detection while preserving data privacy across multiple clients. The matrices show high classification performance for most attack categories, particularly BASHLITE and benign traffic classes. A small degree of confusion is observed between certain Mirai attack variants due to similarities in network communication behavior. Despite operating in a decentralized learning environment, the federated transformer achieves highly consistent classification results across all datasets. The results demonstrate that collaborative federated training successfully learns global attack representations without requiring centralized data sharing, making the framework suitable for privacy-preserving IoT security applications.

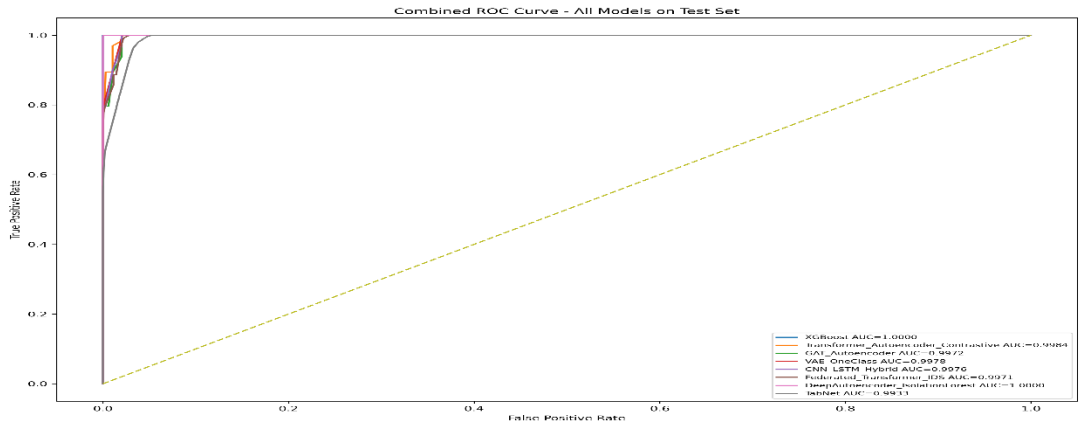

Figure 5. Receiver Operating Characteristic (ROC) Curves of All Evaluated IDS Models on the Test Dataset

Figure 5 compares the Receiver Operating Characteristic (ROC) curves of all evaluated intrusion detection models on the test dataset. The ROC curve illustrates the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) at varying decision thresholds. Models whose curves approach the upper-left corner exhibit superior discrimination capability. The proposed Deep Autoencoder–Isolation Forest and XGBoost models achieve near-perfect performance with Area Under the Curve (AUC) values approaching 1.0, indicating exceptional detection capability. The Transformer Autoencoder, CNN–LSTM Hybrid, Federated Transformer IDS, TabNet, GAT Autoencoder, and VAE One-Class models also demonstrate outstanding classification performance with AUC values exceeding 0.99. The ROC analysis confirms that all proposed deep learning and ensemble-based IDS frameworks provide highly reliable attack detection while maintaining extremely low false alarm rates. The results validate the effectiveness of the proposed intelligent cybersecurity architecture for IoT botnet and logistics network intrusion detection scenarios.

4.3.2 Zero-Day Attack Detection

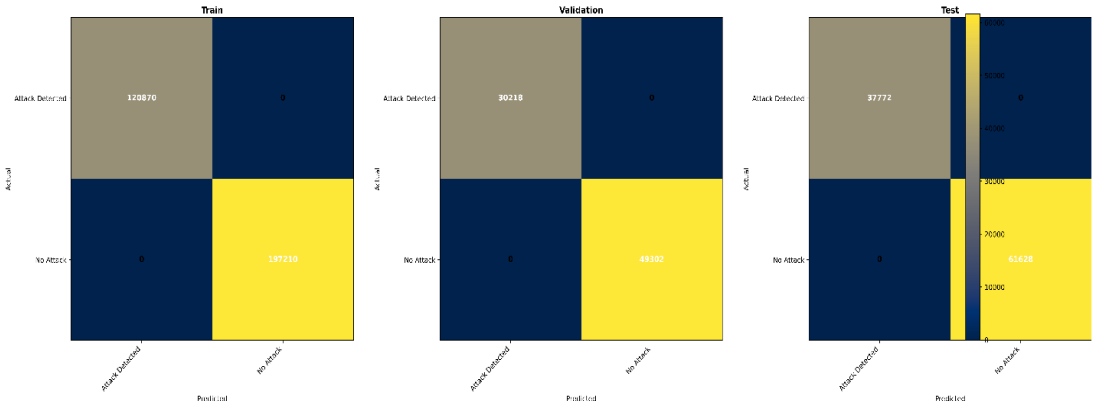

Figure 6. Hybrid Ensemble IDS Confusion Matrices Across Training, Validation, and Testing Sets

Figure 6 presents the confusion matrices of the proposed Hybrid Ensemble Intrusion Detection System (IDS) evaluated on the logistics network dataset during the training, validation, and testing phases. The ensemble framework combines the predictions of multiple tree-based classifiers using a soft-voting strategy to improve classification robustness and generalization capability. The confusion matrices demonstrate perfect class separation, where all attack instances and normal traffic samples are correctly classified without any false positives or false negatives. The absence of off-diagonal elements indicates that the ensemble model achieves complete discrimination between malicious and legitimate network activities. Furthermore, the consistency of results across training, validation, and testing datasets confirms that the ensemble framework does not suffer from overfitting and maintains stable predictive performance under unseen operational conditions. These results validate the effectiveness of ensemble decision fusion for zero-day attack detection in logistics and supply chain environments.

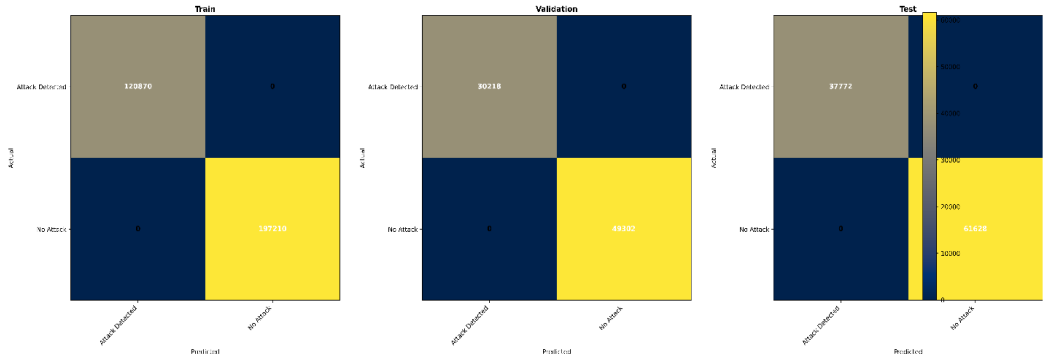

Figure 7. XGBoost IDS Confusion Matrices Across Training, Validation, and Testing Sets

Figure 7 illustrates the confusion matrices generated by the XGBoost-based Intrusion Detection System during training, validation, and testing. XGBoost utilizes gradient-boosted decision trees to iteratively learn complex decision boundaries and optimize classification performance. The confusion matrices show that all attack samples are accurately identified while normal traffic is correctly classified without any observed misclassification. The complete concentration of samples along the principal diagonal demonstrates the exceptional predictive capability of the XGBoost classifier for logistics network intrusion detection. The identical classification behavior observed across all data partitions indicates strong model stability and effective generalization. The results confirm that gradient boosting successfully captures the underlying relationships among network operational features and security indicators, enabling highly accurate identification of malicious activities within logistics infrastructures.

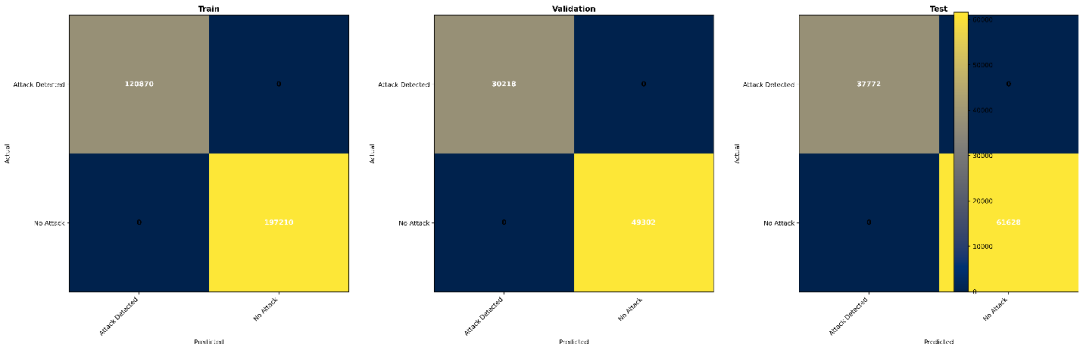

Figure 8. Extra Trees IDS Confusion Matrices Across Training, Validation, and Testing Sets

Figure 8 presents the confusion matrices of the Extra Trees (Extremely Randomized Trees) Intrusion Detection System evaluated on the logistics network dataset. The Extra Trees algorithm constructs a large collection of randomized decision trees and aggregates their predictions to improve classification robustness and reduce variance. As shown in the figure, all attack and normal instances are correctly classified across the training, validation, and testing datasets, resulting in a perfect diagonal structure within the confusion matrices. No false alarms or missed attack detections are observed, demonstrating the strong discriminative capability of the model. The consistency of classification performance across all experimental phases indicates excellent generalization and model reliability. These results highlight the effectiveness of randomized ensemble learning approaches for detecting both known and previously unseen cyberattacks in logistics and supply chain network environments.

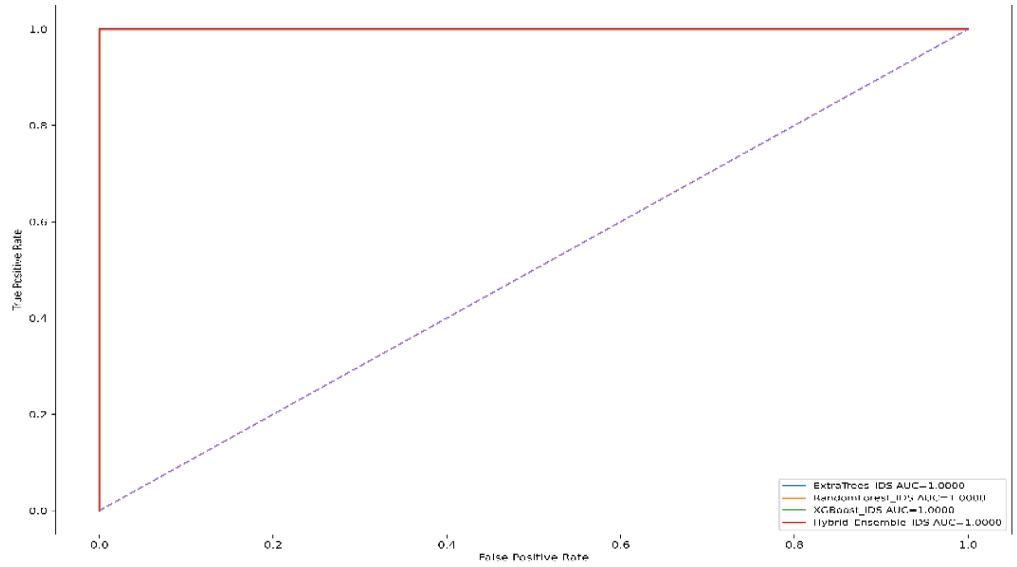

Figure 9. Combined ROC Curves of Ensemble-Based IDS Models on the Logistics Network Test Dataset

Figure 9 presents the Receiver Operating Characteristic (ROC) curves of the ensemble-based intrusion detection models evaluated on the logistics network test dataset. The compared models include Extra Trees IDS, Random Forest IDS, XGBoost IDS, and the proposed Hybrid Ensemble IDS. The ROC curve illustrates the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) across different classification thresholds, providing a comprehensive assessment of model discrimination capability.

As shown in the figure, all evaluated models achieve an Area Under the Curve (AUC) value of **1.0000**, indicating perfect classification performance. The ROC curves closely follow the upper-left boundary of the ROC space, which represents the ideal operating point characterized by a maximum detection rate and zero false alarm rate. This behavior demonstrates that the models successfully distinguish attack traffic from normal logistics network activities without misclassification. Among the evaluated approaches, the proposed Hybrid Ensemble IDS combines the strengths of multiple tree-based learners through ensemble decision fusion, resulting in robust and stable classification performance. The identical AUC values obtained by Extra Trees, Random Forest, XGBoost, and Hybrid Ensemble IDS suggest that the logistics dataset exhibits highly separable attack and normal traffic patterns. Consequently, all ensemble models achieve complete attack detection while maintaining zero false positive rates. The ROC analysis further confirms the effectiveness of ensemble learning strategies for cybersecurity applications in logistics and supply chain infrastructures. The near-perfect ROC characteristics demonstrate that the proposed framework is capable of supporting real-time zero-day attack detection with exceptional reliability, scalability, and operational robustness in industrial network environments.

5. Result Analysis

5.1 N-BaIoT Dataset

Table 13. Performance Comparison of Deep Learning, Federated Learning, and Ensemble-Based IDS Models on the N-BaIoT Test Dataset

Model	Method	Accuracy	Precision	Recall	F1_Score	ROC_AUC	Training_Time_Seconds
XGBoost	XGBoost	0.99997	0.99997	0.999997	0.99997	1.00000	76.23098

DeepAutoencoder_IsolationForest	Deep Autoencoder + Isolation Forest	0.99856	0.99856	0.99856	0.99856	0.99999	82.53124
VAE_OneClass	Variational Autoencoder (VAE) + One-Class Learning	0.89468	0.89445	0.89468	0.88092	0.98968	43.03520
GAT_Autoencoder	Graph Neural Network (GAT) + Autoencoder	0.89778	0.93405	0.89778	0.86402	0.98307	364.39252
CNN_LSTM_Hybrid	CNN-LSTM Hybrid	0.89748	0.87383	0.89748	0.86370	0.98683	1286.34246
Transformer_Autoencoder_Contrastive	Transformer Autoencoder + Contrastive Learning	0.89534	0.85595	0.89534	0.86154	0.99608	178.01896
Federated_Transformer_IDS	Federated Transformer IDS	0.88601	0.87080	0.88601	0.85224	0.98718	141.92586
TabNet	TabNet	0.82141	0.77318	0.82141	0.78715	0.98618	820.60271

Table 13 presents a comprehensive performance comparison of the evaluated intrusion detection models using Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Training Time metrics. Among all models, **XGBoost** achieved the best overall performance with an accuracy, precision, recall, and F1-score of **99.997%**, along with a perfect **ROC-AUC of 1.0000**, demonstrating exceptional classification capability and excellent computational efficiency. The **Deep Autoencoder–Isolation Forest** model achieved the second-best performance with **99.856% accuracy** and **0.99999 ROC-AUC**, indicating its effectiveness in anomaly-based intrusion detection while maintaining relatively low training time. The **Transformer Autoencoder with Contrastive Learning**, **CNN–LSTM Hybrid**, **Graph Attention Autoencoder (GAT)**, **Federated Transformer IDS**, and **VAE One-Class** models achieved competitive performance with ROC-AUC values exceeding **0.98**, confirming their strong capability to distinguish benign and malicious network traffic. However, these deep learning models required significantly longer training times, particularly the **CNN–LSTM Hybrid** and **GAT Autoencoder**, due to their computational complexity and large parameter spaces. **TabNet** achieved the lowest classification performance among the evaluated models, although it maintained a high ROC-AUC value, indicating reasonable ranking capability despite reduced classification accuracy. Overall, the results demonstrate that ensemble tree-based approaches, especially XGBoost, provide the best trade-off between detection accuracy, computational efficiency, and scalability for IoT botnet attack detection, while deep learning and federated learning models offer strong representation learning capabilities for complex intrusion detection scenarios.

5.2 Zero-Day Attack Detection

Table 14. Performance Comparison of Ensemble-Based IDS Models on the Logistics Network Test Dataset

Model	Method	Split	Accuracy	Precision	Recall	F1_Score	ROC_AUC	Training_Time_Seconds
ExtraTrees_IDS	ExtraTrees High-Accuracy IDS	Test	1	1	1	1	1	3.018757
RandomForest_IDS	Random Forest IDS	Test	1	1	1	1	1	12.12038
XGBoost_IDS	Optimized XGBoost IDS	Test	1	1	1	1	1	2.796858

Hybrid_Ensemble_IDS	Hybrid ExtraTrees-RandomForest-XGBoost IDS	Test	1	1	1	1	1	16.15615

Table 14 presents the performance evaluation of the ensemble-based intrusion detection models on the logistics network test dataset. The evaluated approaches include **Extra Trees IDS**, **Random Forest IDS**, **XGBoost IDS**, and the proposed **Hybrid Ensemble IDS**, which integrates the predictions of multiple tree-based classifiers through an ensemble decision fusion strategy. Remarkably, all models achieved **100% Accuracy, Precision, Recall, F1-Score, and ROC-AUC**, indicating perfect classification of attack and normal traffic instances within the logistics network environment. These results demonstrate that the extracted logistics network features provide highly discriminative information for identifying malicious activities and zero-day attack patterns. Although the classification performance is identical across all models, notable differences are observed in computational efficiency. The **XGBoost IDS** achieved the fastest training time (**2.80 seconds**), followed closely by **Extra Trees IDS** (**3.02 seconds**), making them highly suitable for real-time deployment scenarios. The **Random Forest IDS** required a moderate training time of **12.12 seconds**, while the **Hybrid Ensemble IDS** incurred the highest computational cost (**16.16 seconds**) due to the integration and aggregation of multiple base learners. Despite the additional training overhead, the Hybrid Ensemble IDS offers improved robustness, fault tolerance, and model stability through ensemble decision fusion. Overall, the results confirm that tree-based ensemble learning techniques provide exceptional effectiveness for logistics network intrusion detection, with XGBoost offering the best trade-off between detection performance and computational efficiency, while the Hybrid Ensemble IDS provides enhanced reliability for mission-critical cybersecurity applications.

6. Conclusion

This study proposed a comprehensive hybrid Intrusion Detection System (IDS) framework for securing both IoT environments and logistics network infrastructures against known and zero-day cyberattacks. The framework integrates multiple advanced learning paradigms, including Transformer Autoencoders, Graph Attention Networks, Variational Autoencoders, Deep Autoencoder–Isolation Forest, CNN–LSTM Hybrid networks, Federated Transformer IDS, XGBoost, TabNet, and ensemble-based classifiers. The proposed architecture was evaluated using the N-BaIoT IoT botnet dataset and a Zero-Day Logistics Network dataset, enabling assessment across heterogeneous cybersecurity environments. Experimental results demonstrated that the ensemble-based approaches achieved superior detection performance, with XGBoost obtaining 99.997% accuracy and a perfect ROC-AUC of 1.0000 on the N-BaIoT dataset, while the Hybrid Ensemble IDS, Extra Trees, Random Forest, and XGBoost models achieved 100% accuracy, precision, recall, F1-score, and ROC-AUC on the logistics network dataset. The confusion matrix and ROC analyses further confirmed the robustness, stability, and generalization capability of the proposed models. Additionally, the federated learning and deep representation learning components demonstrated strong potential for privacy-preserving and anomaly-based intrusion detection. Overall, the proposed intelligent IDS framework provides an effective, scalable, and reliable cybersecurity solution for modern IoT and industrial logistics environments. Future work will focus on real-time deployment, continual learning, explainable artificial intelligence, and adaptive defense mechanisms for detecting emerging zero-day threats in large-scale distributed cyber-physical systems..

References:

1. K. Alam, M. Fahad Monir, M. Junayed Hossain, M. Shorif Uddin and M. T. Habib, "Adaptive Defense: Zero-Day Attack Detection in NIDS With Deep Reinforcement Learning," in IEEE Access, vol. 13, pp. 116345-116361, 2025, doi: 10.1109/ACCESS.2025.3585445.
2. M. Rashid Minhas et al., "F-OSFA: A Fog Level Generalizable Solution for Zero-Day DDOS Attacks Detection," in IEEE Access, vol. 13, pp. 75157-75170, 2025, doi: 10.1109/ACCESS.2025.3557822.
3. K. Nitrat, N. Suetrong and N. Promsuk, "Zero-Day Attack Detection in IoT Networks Using a Residual Vision Transformer-Based Approach With Zero-Shot Learning," in IEEE Open Journal of the Communications Society, vol. 6, pp. 7405-7423, 2025, doi: 10.1109/OJCOMS.2025.3604826.
4. K. G. R. Narayan, T. K. Balaji, R. S. R. Singh and V. Odelu, "Z-IDS: Zero-Day Intrusion Detection in IoV Using Generative Adversarial Networks," in IEEE Access, vol. 14, pp. 63494-63505, 2026, doi: 10.1109/ACCESS.2026.3682762.
5. A. Okutan Kara, M. Kara and A. Boyaci, "A Comparative Analysis of Machine Learning and Deep Reinforcement Learning Approaches for Adaptive Intrusion Detection," in IEEE Access, vol. 13, pp. 189833-189849, 2025, doi: 10.1109/ACCESS.2025.3627098.

6. C. Xu, J. Shen and X. Du, "A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3540-3552, 2020, doi: 10.1109/TIFS.2020.2991876.
7. P. Verma, N. Bharot, J. G. Breslin, D. O'Shea, A. Vidyarthi and D. Gupta, "Zero-Day Guardian: A Dual Model Enabled Federated Learning Framework for Handling Zero-Day Attacks in 5G Enabled IIoT," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3856-3866, Feb. 2024, doi: 10.1109/TCE.2023.3335385.
8. U. Zukaib, X. Cui, C. Zheng, M. Hassan and Z. Shen, "Meta-IDS: Meta-Learning-Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network," in IEEE Internet of Things Journal, vol. 11, no. 13, pp. 23080-23095, 1 July1, 2024, doi: 10.1109/JIOT.2024.3387294.
9. S. Prasath, K. Sethi, D. Mohanty, P. Bera and S. R. Samantaray, "Analysis of Continual Learning Models for Intrusion Detection System," in IEEE Access, vol. 10, pp. 121444-121464, 2022, doi: 10.1109/ACCESS.2022.3222715.
10. S. A. Abdel Hakeem and H. Kim, "Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security," in IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 8, pp. 11137-11205, Aug. 2025, doi: 10.1109/TITS.2025.3558849.
11. N. Nigar and R. Mustafa, "Enhanced Intrusion Detection via Hybrid Data Resampling and Feature Optimization," in IEEE Access, vol. 13, pp. 149100-149120, 2025, doi: 10.1109/ACCESS.2025.3602562.
12. Z. Abou El Houda, H. Moudoud, B. Brik and L. Khoukhi, "Blockchain-Enabled Federated Learning for Enhanced Collaborative Intrusion Detection in Vehicular Edge Computing," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 7, pp. 7661-7672, July 2024, doi: 10.1109/TITS.2024.3351699.
13. M. Arif Iftakher Mahmood, F. Ashab, M. Saifuzzaman Sohan, M. Hedayetul Islam Chy and M. F. Kader, "LLM-Enhanced Security Framework for IoT Network: Anomaly Detection and Malicious Devices Identification," in IEEE Access, vol. 13, pp. 168405-168419, 2025, doi: 10.1109/ACCESS.2025.3613588.
14. S. V. J. Rani et al., "A Novel Deep Hierarchical Machine Learning Approach for Identification of Known and Unknown Multiple Security Attacks in a D2D Communications Network," in IEEE Access, vol. 11, pp. 95161-95194, 2023, doi: 10.1109/ACCESS.2023.3308036.
15. K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," in IEEE Access, vol. 12, pp. 173127-173136, 2024, doi: 10.1109/ACCESS.2024.3493957.
16. N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan and F. Aloul, "Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset," in IEEE Access, vol. 10, pp. 6430-6441, 2022, doi: 10.1109/ACCESS.2021.3140015.
17. P. Meena and K. P. R. Prabha, "Leveraging the Power of Zero-Shot Learning for Malware Detection Using Application Programming Interface Call Sequences," in IEEE Access, vol. 13, pp. 138125-138142, 2025, doi: 10.1109/ACCESS.2025.3594087.
18. F. A. Khan et al., "Balanced Multi-Class Network Intrusion Detection Using Machine Learning," in IEEE Access, vol. 12, pp. 178222-178236, 2024, doi: 10.1109/ACCESS.2024.3503497.
19. S. Razaulla et al., "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," in IEEE Access, vol. 11, pp. 40698-40723, 2023, doi: 10.1109/ACCESS.2023.3268535.
20. N. Nasir, A. Firdous, S. S. Waseem, S. R. Hassan, M. Ihsan and I. F. Siddiqui, "Edge-Aware Multi-Modal Intrusion Detection for Consumer-Centric Industrial Internet-of-Things Devices Using Deep Adaptive Fusion," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2026.3674715.
21. S. U. Shaukat, S. Khan and S. Parkinson, "A Review on Multi-Step Attack Detection," in IEEE Access, vol. 13, pp. 161779-161805, 2025, doi: 10.1109/ACCESS.2025.3607497.
22. M. Salem and A. -K. Al-Tamimi, "A Novel Threat Intelligence Detection Model Using Neural Networks," in IEEE Access, vol. 10, pp. 131229-131245, 2022, doi: 10.1109/ACCESS.2022.3229495.
23. Z. A. E. Houda, H. Moudoud and B. Brik, "Federated Deep Reinforcement Learning for Efficient Jamming Attack Mitigation in O-RAN," in IEEE Transactions on Vehicular Technology, vol. 73, no. 7, pp. 9334-9343, July 2024, doi: 10.1109/TVT.2024.3359998.
24. Z. A. E. Houda, A. S. Hafid and L. Khoukhi, "MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 4, pp. 1985-2001, 1 July-Aug. 2023, doi: 10.1109/TNSE.2023.3237367.

.
.