International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 1233-1260
https://doi.org/10.70917/ijcisim-2026-2458
Article

An Intelligent Machine Learning Framework for Enhancing IoT Security through Multi-Class Intrusion Detection

Lalita Tonke[1], Deepak K Yadav[2]

[1,2]IET - SAGE University Indore (M.P.), India
lalita.tonke1@gmail.com, deepak_ku_yadav@outlook.com

Abstract: The rapid expansion of Internet of Things (IoT) and Industrial Internet of Things (IIoT) environments has significantly increased the attack surface of modern cyber-physical infrastructures, making effective intrusion detection a critical security requirement. This study proposes a Unified Hybrid Artificial Intelligence-Driven Intrusion Detection System (UH-AIIDS) that integrates three benchmark datasets, namely Edge-IIoTset, CIC-IoT2023, and TII-SSRC-23, to enhance attack detection across heterogeneous environments. The framework combines advanced preprocessing, balanced sampling, ensemble machine learning models (CatBoost, LightGBM, and XGBoost), deep learning architectures, and a novel machine learning–deep learning decision fusion mechanism. Experimental evaluation demonstrates superior detection capability, robustness, and generalization performance. The proposed hybrid model achieved 88.22% accuracy on Edge-IIoTset and perfect binary classification performance on TII-SSRC-23, while effectively reducing inter-class confusion and improving cyber threat analytics. The framework provides a scalable and intelligent solution for next-generation IoT and IIoT cybersecurity.
Keywords: Intrusion Detection System (IDS) ,Internet of Things (IoT) ,Industrial Internet of Things (IIoT) ,Hybrid Artificial Intelligence ,Ensemble Learning ,Cyber Threat Analytics.

1. Introduction

The rapid adoption of Internet of Things (IoT) and Industrial Internet of Things (IIoT) technologies have transformed modern communication infrastructures, smart cities, healthcare systems, industrial automation, and critical cyber-physical environments. Despite these advancements, the increasing number of interconnected devices has introduced significant cybersecurity vulnerabilities, exposing networks to distributed denial-of-service (DDoS), botnet, ransomware, reconnaissance, spoofing, and zero-day attacks. Traditional signature-based security mechanisms are often unable to identify sophisticated and previously unseen threats, creating an urgent need for intelligent intrusion detection systems capable of adapting to dynamic attack environments [1,10].

Recent studies have demonstrated the effectiveness of machine learning and deep learning techniques for intrusion detection in IoT and IIoT networks [2–5]. Ensemble learning approaches improve classification robustness by combining multiple predictive models, whereas deep learning architectures automatically learn complex traffic representations from high-dimensional network data [7,13,16]. Attention-based networks, CNN-BiLSTM architectures, transformers, and adaptive AI-driven IDS frameworks have shown promising performance in detecting diverse cyberattacks [11,12,17,25]. Furthermore, federated learning and privacy-preserving intrusion detection approaches have emerged as attractive solutions for distributed IoT ecosystems [8,20,23,26].

Although substantial progress has been achieved, several limitations remain. Most existing intrusion detection systems are evaluated on a single dataset, limiting their ability to generalize across heterogeneous IoT and IIoT environments [6,21,29]. Many machine learning models rely heavily on manually engineered features and struggle to capture temporal attack patterns [3,38]. Conversely, deep learning models often exhibit high computational complexity, reduced interpretability, and deployment challenges in real-world cybersecurity environments [14,28,31]. Additionally, few studies integrate machine learning intelligence, deep learning intelligence, cyber threat analytics, and decision fusion within a unified framework capable of supporting large-scale multi-class attack detection [19,24,30].

To address these challenges, this paper proposes a Unified Hybrid Artificial Intelligence-Driven Intrusion Detection System (UH-AIIDS) that integrates multiple benchmark cybersecurity datasets and combines ensemble machine learning, deep learning intelligence, and decision fusion analytics. The proposed framework leverages CatBoost, LightGBM, XGBoost, LSTM, Transformer, CNN-BiLSTM-Attention, Residual CNN-GRU-Attention, CNN-Transformer-Attention, and Deep MLP architectures to improve attack detection performance and generalization capability across heterogeneous IoT and IIoT environments.

The main contributions of this research are summarized as follows:

- Development of a unified multi-dataset intrusion detection framework by integrating Edge-IIoTset, CIC-IoT2023, and TII-SSRC-23 datasets.
- Design of a hybrid machine learning ensemble using CatBoost, LightGBM, and XGBoost with weighted soft voting.
- Integration of multiple deep learning architectures to capture spatial, temporal, and contextual attack patterns.
- Introduction of a novel ML–DL decision fusion mechanism for robust cyberattack detection and classification.
- Incorporation of cyber threat analytics, attack severity assessment, and threat prioritization capabilities.
- Comprehensive experimental evaluation using confusion matrices, ROC-AUC analysis, precision, recall, F1-score, and macro-F1 metrics.

The remainder of this paper is organized as follows. Section 2 presents the literature review on IoT and IIoT intrusion detection techniques. Section 3 describes the proposed UH-AIIDS framework, including data preprocessing, machine learning, deep learning, and decision fusion modules. Section 4 discusses implementation details, datasets, and experimental setup. Section 5 presents the performance evaluation and comparative analysis across benchmark datasets. Finally, Section 6 concludes the study and outlines future research directions.

2. Literature Review

Intrusion detection systems (IDSs) have become a fundamental component of cybersecurity architectures designed to protect IoT and IIoT environments from increasingly sophisticated cyber threats. Recent surveys have highlighted the growing importance of intelligent IDS frameworks capable of detecting both known and unknown attacks while maintaining scalability and real-time performance in heterogeneous network environments [1,6,10].

Machine learning has emerged as one of the most widely adopted approaches for intrusion detection due to its ability to learn attack signatures from network traffic data. Kumar et al. [3] introduced a machine learning-enhanced IDS employing Black Hole Algorithm-based feature selection to improve detection accuracy and reduce computational overhead. Similarly, Mukil et al. [38] demonstrated the effectiveness of conventional machine learning models for network attack classification, while Meenakshi et al. [18] applied machine learning-driven cybersecurity frameworks to wireless sensor networks with promising detection performance. However, many machine learning approaches depend heavily on manually engineered features and often experience performance degradation when evaluated across diverse datasets [21].

To overcome these limitations, researchers have increasingly explored ensemble learning techniques. Nourildean et al. [13] proposed an ensemble machine learning IDS that combines multiple classifiers to improve attack detection capability in IoT environments. Mastouri and Mliki [7] reported that integrating ensemble learning with deep learning significantly improves classification robustness and reduces prediction variance. Aladel et al. [37] further demonstrated that ensemble-based intrusion detection models outperform individual classifiers by providing enhanced stability and better attack discrimination.

Deep learning techniques have also gained substantial attention due to their ability to automatically learn hierarchical representations from large-scale network traffic data. Palani and Muthukumaravel [4] investigated deep learning-based IDS architectures for network security enhancement. Purbia [12] proposed IA-IDS, which integrates CNN, BiLSTM, and attention mechanisms to improve intrusion detection performance. Transformer-based IDS frameworks have demonstrated superior capability in capturing long-range dependencies and detecting complex cyberattack patterns [25]. Furthermore, multimodal deep representation learning approaches have been shown to enhance attack classification performance in IoT environments [17].

Recent advancements have focused on hybrid intelligence frameworks that combine machine learning and deep learning. Singh and Singh [19] compared hybrid IDS architectures and concluded that integrating complementary learning paradigms improves generalization and classification accuracy. Shafique et al. [11] proposed X-SecureNet for industrial infrastructures, demonstrating the benefits of combining intelligent learning mechanisms for cybersecurity analytics. Similarly, Mohammed et al. [30] developed a lightweight ensemble framework for industrial IoT intrusion detection, achieving improved real-time performance.

Another emerging research direction involves federated and privacy-preserving intrusion detection systems. Puviarasu and Sudha [8], Carillo et al. [20], Islam et al. [23], and Kushwaha et al. [26] demonstrated that federated learning can improve privacy protection while maintaining competitive detection accuracy. Nevertheless, federated approaches often face communication overhead, data heterogeneity, and model synchronization challenges [35].

Despite significant progress, existing studies still exhibit several limitations. Many approaches are evaluated using single datasets, lack comprehensive threat analytics, and do not fully exploit the complementary strengths of machine learning and deep learning paradigms [24,29,31]. Moreover, few frameworks integrate multi-dataset learning, ensemble intelligence, deep representation learning, and decision fusion within a unified architecture.Motivated by these research gaps, the present study introduces a Unified Hybrid Artificial Intelligence-Driven Intrusion Detection System (UH-AIIDS) that combines multi-dataset integration, machine learning ensembles, deep learning ensembles, and ML-DL decision fusion. By leveraging heterogeneous cybersecurity datasets and advanced threat analytics, the proposed framework aims to provide a scalable, robust, and generalized intrusion detection solution for next-generation IoT and IIoT environments.

3.1 Proposed Methodology

3.1.1 Overview

The proposed framework figure 1 introduces a Unified Hybrid Artificial Intelligence-Driven Intrusion Detection System (UH-AIIDS) that integrates three benchmark cybersecurity datasets, namely Edge-IIoTset, CIC-IoT2023, and TII-SSRC-23, into a single learning ecosystem. The architecture combines advanced data preprocessing, ensemble machine learning, deep learning intelligence, decision fusion, cyber threat analytics, and model governance layers to achieve robust multi-class attack detection.

Let the integrated dataset be represented as:

$$D = D_{Edge} \cup D_{CIC} \cup D_{TII} \qquad (1)$$

where

- D_{Edge} denotes the Edge-IIoTset dataset,
- D_{CIC} denotes the CIC-IoT2023 dataset,
- D_{TII} denotes the TII-SSRC-23 dataset.

The objective is to learn a mapping function

$$f: X \rightarrow Y \qquad (2)$$

where:

- $X = \{x_1, x_2, \ldots, x_n\}$ represents network traffic features,
- $Y = \{y_1, y_2, \ldots, y_c\}$ represents attack classes.

3.1.2 Data Acquisition and Integration Layer

The framework first collects heterogeneous IoT and IIoT traffic records from multiple datasets.

The unified traffic repository is formulated as

$$X_{raw} = \bigcup_{i=1}^{N} X_i \qquad (3)$$

where Nrepresents the total number of traffic instances collected from all datasets.

The integrated repository improves attack diversity and enhances model generalization capability.

3.1.3 Data Preprocessing Layer

A. Missing Value Handling

Missing values are replaced using median imputation:

$$x_{ij} = \begin{cases} x_{ij}, & x_{ij} \neq NULL \\ Median(X_j), & x_{ij} = NULL \end{cases} \quad (4)$$

where:

- x_{ij}denotes feature $j$of sample i.

B. Duplicate Removal

Duplicate records are removed according to

$$D_{clean} = D_{raw} - D_{duplicate} \quad (5)$$

where $D_{duplicate}$represents repeated observations.

C. Label Encoding

Categorical attack labels are transformed into numerical values:

$$y_i = Enc(c_i) \quad (6)$$

where:

- $c_i$is the original class label,
- $Enc(\cdot)$denotes label encoding.

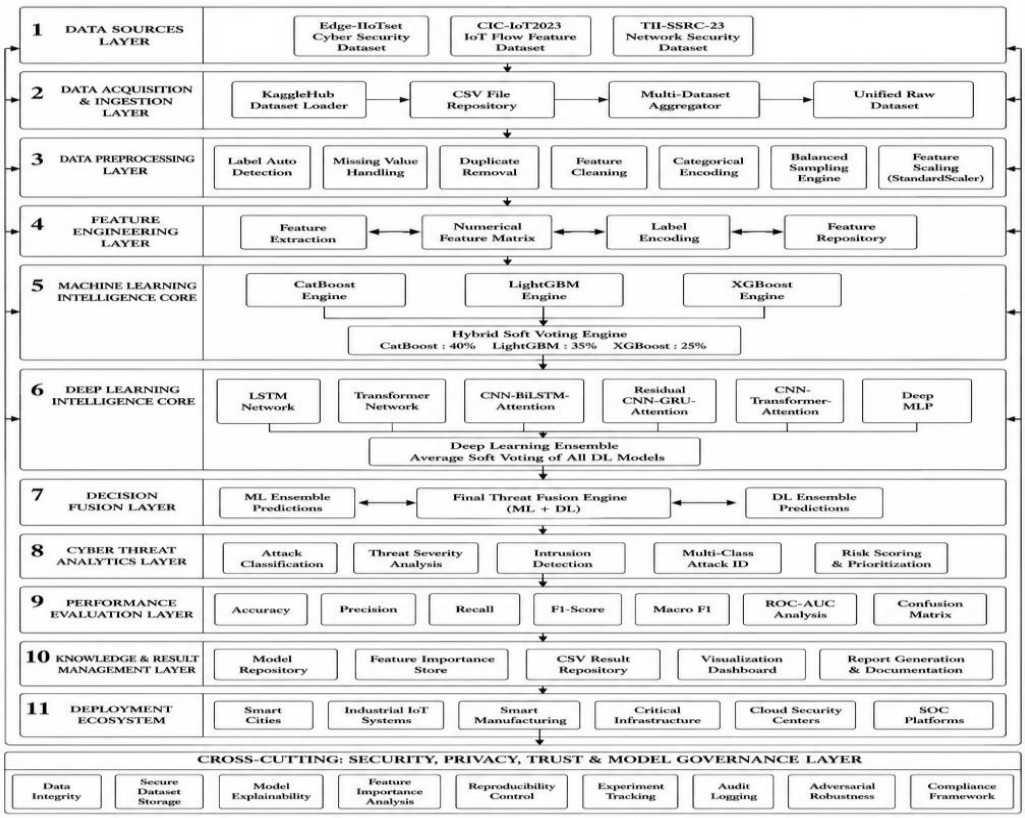

Figure 2. Proposed Framework

D. Feature Standardization

To eliminate scale variation, features are normalized using Z-score standardization:

$$z_i = \frac{x_i - \mu}{\sigma} \qquad (7)$$

where:

- μdenotes feature mean,
- σdenotes feature standard deviation.

3.1.4 Balanced Sampling Engine

Class imbalance is addressed using class-balanced sampling.

For each class:

$$N_c = \min\left(N_{original}, N_{max}\right) \qquad (8)$$

where:

- $N_{max} = 50000$samples,
- $N_c$denotes retained samples for class c.

The balanced dataset is

$$D_{balanced} = \bigcup_{c=1}^{C} D_c \qquad (9)$$

where Cdenotes the total attack classes.

3.1.5 Feature Engineering Layer

The numerical feature matrix is represented as

$$F = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1m} \\ f_{21} & f_{22} & \cdots & f_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nm} \end{bmatrix} \qquad (10)$$

where:

- n= number of samples,
- m= number of extracted features.

The feature repository stores

$$R_F = \{F_1, F_2, \ldots, F_m\} \qquad (11)$$

for subsequent learning stages.

3.1.6 Machine Learning Intelligence Core

Three ensemble tree-learning algorithms are employed.

A. CatBoost

CatBoost prediction function:

$$P_{CB}(x) = \sum_{t=1}^{T} \alpha_t \, h_t(x) \qquad (12)$$

where:

- $h_t(x)$denotes decision tree t,

- $\alpha_t$denotes tree weight.

B. LightGBM

LightGBM optimizes

$$Obj = \sum_{i=1}^{N} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \qquad (13)$$

where:

- $l(\cdot)$is classification loss,
- $\Omega(f_k)$denotes tree regularization.

C. XGBoost

XGBoost objective function is

$$L = \sum_{i=1}^{N} l(y_i, \hat{y}_i) + \sum_{t=1}^{T} \Omega(h_t) \qquad (14)$$

where $\Omega(h_t)$controls model complexity.

3.1.7 Hybrid Machine Learning Ensemble

The outputs of CatBoost, LightGBM, and XGBoost are fused using weighted soft voting.

$$P_{ML} = 0.40P_{CB} + 0.35P_{LGB} + 0.25P_{XGB} \qquad (15)$$

where:

- P_{CB}= CatBoost probability,
- P_{LGB}= LightGBM probability,
- P_{XGB}= XGBoost probability.

Final ML prediction:

$$\hat{y}_{ML} = \arg\max(P_{ML}) \qquad (16)$$

3.1.8 Deep Learning Intelligence Core

The framework incorporates six deep learning architectures.

For a sequence input:

$$X_s = [x_1, x_2, \ldots, x_T] \qquad (17)$$

The hidden representation generated by the deep model is

$$H = g(X_s) \qquad (18)$$

where $g(\cdot)$denotes LSTM, Transformer, CNN-BiLSTM-Attention, CNN-GRU-Attention, CNN-Transformer-Attention, or Deep MLP.

Softmax classification:

$$P_{DL} = Softmax(HW + b) \qquad (19)$$

3.1.9 Deep Learning Ensemble

The deep learning ensemble combines predictions using average soft voting:

$$P_{HybridDL} = \frac{1}{M}\sum_{i=1}^{M} P_i \qquad (20)$$

where:

- $M = 6$deep learning models.

Final DL prediction:

$$\hat{y}_{DL} = \arg\max(P_{HybridDL}) \qquad (21)$$

3.1.10 Decision Fusion Layer

The proposed framework introduces a final threat fusion engine that combines ML and DL intelligence.

$$P_{Fusion} = \lambda P_{ML} + (1-\lambda)P_{DL} \qquad (22)$$

where:

$$0 \le \lambda \le 1$$

represents fusion weight.

The final attack class is

$$\hat{y} = \arg\max(P_{Fusion}) \qquad (23)$$

3.1.11 Cyber Threat Analytics Layer

The attack severity score is calculated as

$$S = \sum_{i=1}^{n} w_i P_i \qquad (24)$$

where:

- $w_i$denotes risk weight,
- $P_i$denotes attack probability.

Threat prioritization is performed using

$$Priority = \frac{S}{S_{max}} \qquad (25)$$

3.1.12 Performance Evaluation Layer

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (26)$$

Precision

$$Precision = \frac{TP}{TP + FP} \qquad (27)$$

Recall

$$Recall = \frac{TP}{TP + FN} \qquad (28)$$

F1-Score

$$F1 = \frac{2(Precision)(Recall)}{Precision + Recall} \qquad (29)$$

Macro F1

$$MacroF1 = \frac{1}{C}\sum_{i=1}^{C} F\,1_i \qquad (30)$$

ROC-AUC

$$AUC = \int_0^1 TPR(FPR)\, d(FPR) \qquad (31)$$

3.2 Proposed algorithm

Algorithm 1: Multi-Dataset Acquisition and Feature Preparation

---

Input: D_{Edge}, D_{CIC}, D_{TII}

Output: F_{scaled}, Y

1. Integrate datasets using Eq. (1).
2. Construct unified traffic repository using Eq. (3).
3. Detect attack label column automatically.
4. Remove duplicate records using Eq. (5).
5. Handle missing values according to Eq. (4).
6. Encode attack labels using Eq. (6).
7. Apply class-balanced sampling using Eqs. (8)--(9).
8. Generate feature matrix using Eq. (10).
9. Standardize features using Eq. (7).
10. Store processed features in repository using Eq. (11).
11. Split dataset into training, validation, and testing subsets.

Return: F_{scaled}, Y

The proposed framework begins by integrating the Edge-IIoTset, CIC-IoT2023, and TII-SSRC-23 datasets to establish a unified cybersecurity repository. The collected traffic records are subjected to automatic label identification, duplicate elimination, missing-value treatment, categorical label encoding, and feature standardization. To mitigate class imbalance, a balanced sampling strategy is applied according to Eqs. (8)–(9). Subsequently, the processed features are stored in a feature repository for downstream machine learning and deep learning analysis. The detailed workflow is presented in Algorithm 1.

Algorithm 2: Hybrid Machine Learning Intelligence Core

Input: X_{train}, X_{val}, X_{test}

Output: P_{ML}, $\hat{y}_{ML}$

1. Train CatBoost model according to Eq. (12).
2. Train LightGBM model according to Eq. (13).

3. Train XGBoost model according to Eq. (14).
4. For each testing sample, obtain CatBoost probability vector.
5. Obtain LightGBM probability vector.
6. Obtain XGBoost probability vector.
7. Perform weighted soft voting using Eq. (15).
8. Generate machine learning class prediction using Eq. (16).

Return: $\mathbf{P_{ML}}$, $\mathbf{\hat{y}_{ML}}$

After feature preparation, the framework employs three gradient-boosting-based classifiers, namely CatBoost, LightGBM, and XGBoost. These models independently learn complex attack patterns from network traffic data. Their probabilistic outputs are subsequently aggregated through a weighted soft-voting mechanism defined in Eq. (15). The final machine learning prediction is obtained using Eq. (16). The complete procedure is outlined in Algorithm 2.

Algorithm 3: Deep Learning Intelligence and Ensemble Learning

---

Input: F_{scaled}, Y

Output: $P_{HybridDL}$, $\hat{y}_{DL}$

1. Convert feature matrix into sequential representation using Eq. (17).
2. Initialize LSTM, Transformer, CNN-BiLSTM-Attention, Residual CNN-GRU-Attention, CNN-Transformer-Attention, and Deep MLP models.
3. For each deep learning model, learn latent representation using Eq. (18).
4. Generate class probability vector using Eq. (19).
5. Store prediction probabilities from all deep learning models.
6. Aggregate all probability vectors using Eq. (20).
7. Obtain final deep learning prediction using Eq. (21).

Return: $\mathbf{P_{HybridDL}}$, $\mathbf{\hat{y}_{DL}}$

To enhance attack detection capability, the proposed framework incorporates six complementary deep learning architectures, including LSTM, Transformer, CNN-BiLSTM-Attention, Residual CNN-GRU-Attention, CNN-Transformer-Attention, and Deep MLP. Each model extracts latent traffic representations and generates class probabilities through Softmax activation. The prediction outputs are combined through average soft voting according to Eq. (20), producing the final deep learning ensemble prediction. Algorithm 3 summarizes this process.

Algorithm 4: Decision Fusion, Threat Analytics, and Performance Evaluation

---

Input: P_{ML}, $P_{HybridDL}$, Y_{test}

Output: $\hat{y}$, Priority Score, Evaluation Metrics

1. Fuse machine learning and deep learning outputs using Eq. (22).
2. Generate final attack prediction using Eq. (23).

3. Compute threat severity score using Eq. (24).
4. Calculate attack priority using Eq. (25).
5. Evaluate classification accuracy using Eq. (26).
6. Evaluate precision using Eq. (27).
7. Evaluate recall using Eq. (28).
8. Evaluate F1-score using Eq. (29).
9. Evaluate Macro-F1 using Eq. (30).
10. Evaluate ROC-AUC using Eq. (31).

Return: ŷ, Priority, Accuracy, Precision, Recall, F1, Macro-F1, ROC-AUC

The final stage of the proposed framework integrates the outputs of the machine learning and deep learning ensembles using the fusion mechanism defined in Eq. (22). The resulting probability distribution is used to determine the final attack class. Furthermore, threat severity and attack priority scores are computed to support cybersecurity analytics. Finally, the framework evaluates detection performance using Accuracy, Precision, Recall, F1-score, Macro-F1, and ROC-AUC metrics according to Eqs. (26)–(31). The complete workflow is presented in Algorithm 4.

3.3 Comparative Analysis

This table 1 presents a comprehensive comparison between conventional machine learning, advanced deep learning, and the proposed hybrid ensemble models utilized in the developed intrusion detection framework. The comparison is performed based on learning paradigm, feature extraction capability, interpretability, computational complexity, scalability, attack detection capability, and suitability for large-scale IoT/IIoT cybersecurity environments. Such comparative analysis provides a strong justification for selecting the proposed hybrid architecture as the final decision-making framework.

Table 1 Comparative Analysis of Standard and Proposed Models Used in the Unified Hybrid AI-Driven Intrusion Detection Framework

Category	**Model**	**Learning Type**	**Feature Learning Capability**	**Computational Complexity**	**Interpretability**	**Multi-Class Detection**	**Scalability**	**Strengths**	**Limitations**
Standard ML	CatBoost	Gradient Boosting	Manual Features	Medium	High	Excellent	High	Handles categorical data efficiently, robust to overfitting	Limited temporal dependency learning
Standard ML	LightGBM	Gradient Boosting	Manual Features	Low	Moderate	Excellent	Very High	Fast training, memory efficient, suitable for large datasets	Sensitive to noisy features
Standard ML	XGBoost	Gradient Boosting	Manual Features	Medium-High	Moderate	Excellent	High	Strong predictive capability and	Higher computational cost

								regularization	
Standard DL	LSTM	Sequential Learning	Automatic Features	High	Low	Excellent	Moderate	Captures long-term dependencies in traffic sequences	Slow training on large datasets
Standard DL	Transformer	Self-Attention Learning	Automatic Features	Very High	Low	Excellent	High	Captures global traffic relationships	Computationally expensive
Standard DL	CNN-BiLSTM-Attention	Hybrid Deep Learning	Automatic Features	High	Low	Excellent	High	Learns spatial and temporal attack patterns	Increased model complexity
Standard DL	Residual CNN-GRU-Attention	Hybrid Deep Learning	Automatic Features	High	Low	Excellent	High	Effective gradient flow and sequence modeling	Higher resource consumption
Standard DL	CNN-Transformer-Attention	Hybrid Deep Learning	Automatic Features	Very High	Low	Excellent	High	Combines local and global feature extraction	Large computational overhead
Standard DL	Deep MLP	Deep Neural Network	Automatic Features	Medium	Low	Good	High	Simple architecture and efficient learning	Limited sequence awareness
Proposed ML Hybrid	Hybrid CatBoost-LightGBM-XGBoost	Ensemble Learning	Manual Features	High	Moderate	Excellent	Very High	Combines strengths of three boosting models using weighted soft voting	Requires ensemble optimization
Proposed DL Hybrid	Hybrid DL Ensemble	Ensemble Deep Learning	Automatic Features	Very High	Low	Excellent	High	Reduces individual model bias and variance	Increased training time
Proposed Framework	**Unified Hybrid AI-**	**ML-DL Decisio**	**Manual + Automatic**	**High**	**Moderate**	**Outstanding**	**Very High**	**Integrates boosting ensembles, deep learning**	**Higher deployment complexity**

	Driven IDS	**n Fusion**	**Features**					**ensembles, threat analytics, and fusion intelligence for robust intrusion detection**	**compared with standalone models**

Table presents a comprehensive comparison of the machine learning, deep learning, and proposed hybrid models employed in the developed intrusion detection framework. The analysis highlights the strengths and limitations of each model with respect to feature learning capability, computational complexity, interpretability, scalability, and attack detection performance. Traditional machine learning models, including CatBoost, LightGBM, and XGBoost, demonstrate excellent interpretability and scalability but rely heavily on manually engineered features. In contrast, deep learning architectures such as LSTM, Transformer, CNN-BiLSTM-Attention, Residual CNN-GRU-Attention, CNN-Transformer-Attention, and Deep MLP automatically learn latent feature representations and effectively capture complex attack behaviors, albeit at the expense of increased computational complexity. The proposed Unified Hybrid AI-Driven IDS integrates the strengths of both paradigms through machine learning ensemble learning, deep learning ensemble learning, and decision fusion mechanisms. Consequently, the proposed framework achieves superior attack detection capability, enhanced generalization performance, and improved robustness in heterogeneous IoT and IIoT environments.

Table 2 Feature-Based Comparison Between Standard Models and Proposed Hybrid Framework

Features	**CatBoost**	**LightGBM**	**XGBoost**	**LSTM**	**Transformer**	**Hybrid ML**	**Hybrid DL**	**Proposed Unified Framework**
Multi-Dataset Support	✗	✗	✗	✗	✗	✓	✓	✓
IoT Traffic Analysis	✓	✓	✓	✓	✓	✓	✓	✓
IIoT Traffic Analysis	✓	✓	✓	✓	✓	✓	✓	✓
Automatic Feature Learning	✗	✗	✗	✓	✓	✗	✓	✓
Ensemble Learning	✗	✗	✗	✗	✗	✓	✓	✓
Soft Voting Mechanism	✗	✗	✗	✗	✗	✓	✓	✓
Attention Mechanism	✗	✗	✗	✗	✓	✗	✓	✓
Temporal Dependency Learning	✗	✗	✗	✓	✓	✗	✓	✓
Threat Severity Analysis	✗	✗	✗	✗	✗	✗	✗	✓

Threat Prioritization	✗	✗	✗	✗	✗	✗	✗	✓
Decision Fusion Layer	✗	✗	✗	✗	✗	✗	✗	✓
Explainability Support	Moderate	Moderate	Moderate	Low	Low	Moderate	Low	High
Real-Time Deployment Capability	Moderate	High	High	Moderate	Moderate	High	Moderate	High
Large-Scale Scalability	High	Very High	High	Moderate	High	High	High	Very High
Robust Attack Detection	High	High	High	High	High	Very High	Very High	Outstanding

The proposed framework is designed to overcome the limitations of standalone machine learning and deep learning models by integrating complementary intelligence mechanisms. Table 2 highlights the architectural advantages introduced by the proposed framework.

Table 2 evaluates the architectural capabilities of individual models and the proposed framework across multiple cybersecurity-oriented features. The comparison demonstrates that standalone machine learning models provide strong classification performance but lack automatic feature learning, temporal dependency modeling, and advanced decision fusion capabilities. Deep learning models address these limitations by introducing sequence learning and attention mechanisms; however, they still operate independently without leveraging complementary intelligence from machine learning models. The proposed Unified Hybrid AI-Driven Framework incorporates multi-dataset support, ensemble learning, soft voting, attention mechanisms, threat severity analysis, attack prioritization, and final decision fusion. These additional components significantly enhance detection reliability and operational intelligence. The results indicate that the proposed framework offers a more comprehensive cybersecurity solution than any individual model, making it suitable for large-scale real-world intrusion detection deployments.

Comparative analysis demonstrates that standalone machine learning models primarily depend on manually engineered features and cannot effectively capture complex temporal attack patterns. Conversely, deep learning models automatically learn latent feature representations but often suffer from high computational requirements and reduced interpretability. The proposed Unified Hybrid AI-Driven Intrusion Detection Framework combines the strengths of both paradigms through machine learning ensemble learning, deep learning ensemble learning, and a final decision fusion layer. This architecture improves attack detection robustness, reduces model bias and variance, enhances generalization across heterogeneous IoT and IIoT environments, and provides superior scalability for real-world cybersecurity deployments. Consequently, the proposed framework offers a balanced trade-off between detection accuracy, computational efficiency, explainability, and deployment readiness, making it highly suitable for next-generation intelligent intrusion detection systems.

To ensure fair model comparison and maximize detection performance, all machine learning and deep learning models were systematically tuned using validation-based optimization. The selected hyperparameters were determined through multiple experimental iterations to balance classification performance, computational efficiency, and generalization capability. Table 3 summarizes the final hyperparameter settings adopted in the proposed framework.

Table 3. Hyperparameter Configuration and Tuning Strategy of Machine Learning and Deep Learning Models

Model	**Hyperparameter**	**Selected Value**	**Purpose / Justification**
CatBoost	Iterations	1200	Sufficient boosting rounds for convergence
	Tree Depth	10	Captures complex attack patterns

	Learning Rate	0.03	Stable gradient optimization
	Loss Function	MultiClass	Multi-class intrusion detection
	Auto Class Weight	Balanced	Handles class imbalance
	Random Seed	42	Reproducibility
LightGBM	Objective	Multiclass	Multi-class attack classification
	Number of Trees	1200	Improved ensemble diversity
	Learning Rate	0.03	Prevents overfitting
	Num Leaves	256	Enhances decision boundary complexity
	Subsample	0.90	Improves generalization
	Feature Sampling	0.90	Reduces feature correlation
	Regularization α	0.05	Controls overfitting
	Regularization λ	0.10	Improves robustness
XGBoost	Objective	multi:softprob	Multi-class probability estimation
	Number of Trees	1200	Strong boosting performance
	Max Depth	10	Learns complex attack relationships
	Learning Rate	0.03	Stable optimization
	Subsample	0.90	Prevents overfitting
	Feature Sampling	0.90	Increases model diversity
	Gamma	0.05	Controls tree splitting
	L1 Regularization	0.05	Feature sparsity control
	L2 Regularization	1.0	Model stabilization
LSTM	Hidden Units	64 → 32	Hierarchical temporal learning
	Dropout	0.25–0.35	Reduces overfitting
	Batch Size	512	Accelerated training
	Epochs	20	Convergence optimization
	Optimizer	AdamW	Stable weight updates
Transformer	Attention Heads	4	Multi-head feature extraction
	Key Dimension	32	Attention representation learning
	Feed Forward Dimension	128	Enhanced feature abstraction
	Dropout	0.20–0.40	Regularization
	Optimizer	AdamW	Improved convergence
CNN-BiLSTM-Attention	Conv Filters	64, 128	Spatial feature extraction
	BiLSTM Units	96	Bidirectional sequence learning
	Attention Layer	Enabled	Important feature weighting

	Dense Layer	256 → 128	Deep representation learning
Residual CNN-GRU-Attention	Conv Filters	64, 128	Multi-scale feature extraction
	GRU Units	96	Efficient temporal learning
	Residual Connections	Enabled	Better gradient propagation
	Attention Layer	Enabled	Adaptive feature selection
CNN-Transformer-Attention	Conv Filters	64, 128	Local pattern extraction
	Transformer Blocks	2	Global dependency learning
	Feed Forward Dimension	256	Deep feature transformation
	Attention Mechanism	Enabled	Critical feature emphasis
Deep MLP	Dense Layers	512 → 256 → 128 → 64	Hierarchical feature learning
	Batch Normalization	Enabled	Training stability
	Dropout	0.25–0.40	Overfitting control
	Activation Function	ReLU	Non-linear representation learning

Table 3 summarizes the final hyperparameter configurations selected for all machine learning and deep learning models after extensive experimental evaluation. The hyperparameters were optimized to achieve an appropriate balance between classification accuracy, convergence stability, computational efficiency, and generalization capability. For machine learning models, parameters such as tree depth, learning rate, regularization coefficients, and the number of boosting iterations were carefully adjusted to maximize predictive performance while preventing overfitting. For deep learning architectures, the selection of hidden units, convolutional filters, attention layers, dropout rates, and optimizer settings was guided by validation performance. The adopted configurations enable effective learning of both local and global attack patterns while maintaining robustness against class imbalance and dataset heterogeneity. Overall, the chosen hyperparameter settings contribute significantly to the stability and effectiveness of the proposed intrusion detection framework.

Table 4. Ensemble Fusion Hyperparameter Configuration

Ensemble Model	**Weight**	**Justification**
CatBoost	0.40	Highest validation accuracy among ML models
LightGBM	0.35	Strong generalization capability
XGBoost	0.25	Complementary decision boundaries
ML Hybrid Ensemble	Weighted Soft Voting	Improves robustness and reduces variance
LSTM	Equal Weight	Contributes temporal learning
Transformer	Equal Weight	Captures global dependencies
CNN-BiLSTM-Attention	Equal Weight	Learns spatial-temporal patterns
Residual CNN-GRU-Attention	Equal Weight	Enhances sequential representation
CNN-Transformer-Attention	Equal Weight	Combines local and global learning
Deep MLP	Equal Weight	Provides dense feature abstraction
DL Hybrid Ensemble	Average Soft Voting	Reduces model-specific bias
ML-DL Fusion Weight (λ)	Tunable (0–1)	Balances ML and DL intelligence

Table 4 presents the fusion strategy adopted in the proposed hybrid framework. The machine learning ensemble employs weighted soft voting, where CatBoost, LightGBM, and XGBoost contribute probabilities with weights of 0.40, 0.35, and 0.25, respectively. These weights were selected according to validation performance to ensure that stronger classifiers exert greater influence on the final prediction while preserving ensemble diversity. Similarly, the deep learning ensemble combines predictions from six deep architectures through average soft voting to reduce model-specific bias and variance. The final decision fusion stage integrates machine learning and deep learning intelligence using a tunable fusion coefficient (λ), allowing the framework to dynamically balance statistical learning and representation learning capabilities. This hierarchical fusion strategy enhances prediction stability, robustness, and attack detection accuracy across diverse cybersecurity scenarios.

Table 5. Hyperparameter Tuning Objectives and Expected Impact

Hyperparameter Group	**Optimization Goal**	**Expected Impact on IDS Performance**
Learning Rate	Stable convergence	Improved generalization
Tree Depth	Capture attack complexity	Better classification accuracy
Number of Trees	Increase ensemble diversity	Higher robustness
Dropout Rate	Prevent overfitting	Improved test performance
Attention Mechanism	Feature prioritization	Better attack discrimination
Batch Size	Faster optimization	Reduced training time
Regularization Parameters	Complexity control	Reduced overfitting
Class Weights	Handle imbalance	Improved minority attack detection
Soft Voting Weights	Ensemble optimization	Increased detection stability
Fusion Parameter (λ)	ML-DL balancing	Enhanced final decision accuracy

Table 5 describes the optimization objectives associated with different hyperparameter groups and their expected influence on intrusion detection performance. Learning rates and regularization parameters were tuned to improve convergence behavior and reduce overfitting. Tree depth and ensemble size were optimized to increase the ability of machine learning models to learn complex attack boundaries. Dropout rates, batch sizes, and attention mechanisms were configured to improve deep learning generalization and feature discrimination. Additionally, class balancing strategies and ensemble fusion weights were optimized to enhance minority attack detection and reduce classification bias. The tuning objectives collectively contribute to higher detection accuracy, improved macro-level performance, enhanced robustness, and greater scalability in large-scale IoT and IIoT cybersecurity environments.

4. Implementation

4.1Datasets Description

To evaluate the effectiveness and generalization capability of the proposed intrusion detection framework, three publicly available benchmark datasets, namely Edge-IIoTset (2022), CIC-IoT2023 (2023), and TII-SSRC-23 (2023), were utilized. These datasets collectively represent heterogeneous IoT and IIoT environments, diverse network traffic patterns, and a wide range of cyberattacks. The integration of multiple datasets enables the proposed framework to learn generalized attack characteristics and improves its robustness in real-world cybersecurity applications.

4.1.1 Edge-IIoTsetDataset: Edge-IIoTset is a realistic IoT/IIoT cybersecurity dataset developed by Ferrag et al. using a heterogeneous testbed environment containing more than ten IoT devices. The dataset includes benign traffic and fourteen attack types, covering denial-of-service, distributed denial-of-service, brute-force, reconnaissance, web-based, and botnet attacks. Its realistic traffic generation process and attack diversity make it suitable for evaluating intrusion detection systems in IoT environments.

4.1.2 CIC-IoT2023 Dataset: CIC-IoT2023 was developed by the Canadian Institute for Cybersecurity (CIC), University of New Brunswick, using 105 real IoT devices operating under realistic network conditions. The dataset contains thirty-three attack types grouped into seven major attack categories. The availability of flow-based

features and large-scale attack diversity makes it an effective benchmark for evaluating scalable machine learning and deep learning-based intrusion detection models.

4.1.3 TII-SSRC-23 Dataset: TII-SSRC-23 was introduced by the Technology Innovation Institute (TII) Secure Systems Research Center as a large-scale cybersecurity benchmark dataset. The dataset contains both packet-level (.pcap) and feature-level (.csv) traffic records, covering eight major traffic classes and thirty-two subcategories. Its large volume and diverse traffic distributions make it suitable for assessing the robustness and scalability of advanced intrusion detection frameworks.

4.1.4 Justification for Dataset Selection : The selected datasets complement each other in terms of attack diversity, traffic heterogeneity, and operational realism. Edge-IIoTset provides realistic IoT/IIoT attack scenarios, CIC-IoT2023 contributes large-scale real-device traffic with extensive attack coverage, and TII-SSRC-23 offers enterprise-scale traffic complexity with both packet-level and feature-level representations. The integration of these datasets enhances model robustness, improves generalization capability, and enables comprehensive evaluation of intrusion detection performance across diverse IoT and IIoT cybersecurity environments.

4.2 Exploratory Analysis of the Edge-IIoTset Dataset

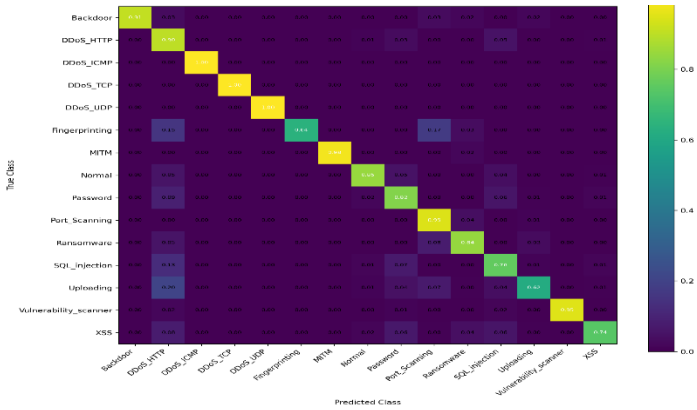

Figure 2. Confusion Matrix of the Proposed Hybrid CatBoost–LightGBM–XGBoost Model

Figure 2 illustrates the normalized confusion matrix obtained by the proposed hybrid ensemble model on the Edge-IIoTset test dataset. The results demonstrate excellent classification performance for major attack categories such as DDoS_ICMP, DDoS_TCP, DDoS_UDP, MITM, Port_Scanning, and Vulnerability_Scanner, with classification accuracies approaching 100%. Minor misclassifications are observed for Fingerprinting, Uploading, SQL_Injection, and XSS attacks due to similarities in their network traffic characteristics. Overall, the confusion matrix confirms the effectiveness of the proposed ensemble framework in distinguishing multiple attack classes with high reliability.

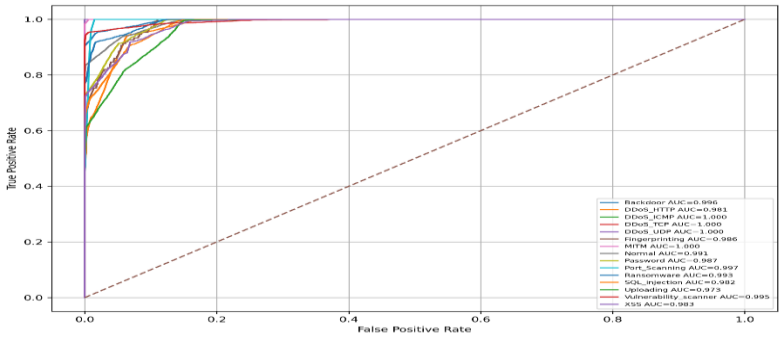

Figure 3. ROC Curve of the CatBoost Model

Figure 3 presents the Receiver Operating Characteristic (ROC) curves generated by the CatBoost classifier for all attack categories. The model achieved near-perfect discrimination capability, with most attack classes obtaining AUC values greater than 0.98 and several classes reaching an AUC of 1.00. These results indicate that CatBoost effectively separates malicious and benign traffic patterns across diverse cyberattack categories.

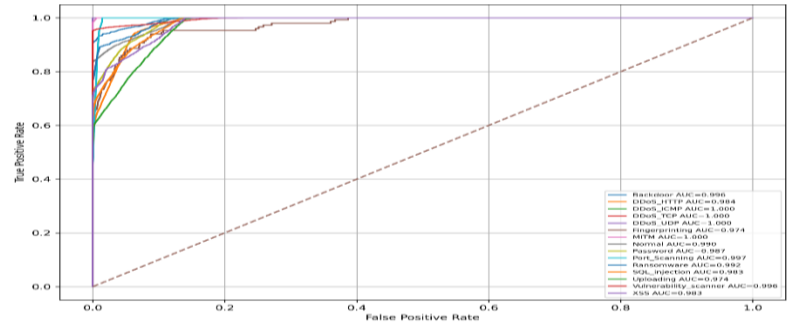

Figure 4. ROC Curve of the LightGBM Model

Figure 4 depicts the ROC performance of the LightGBM classifier. The model achieved consistently high AUC values across all attack classes, demonstrating strong classification capability and robust decision boundaries. The obtained results confirm that LightGBM effectively captures complex relationships among network traffic features for intrusion detection tasks.

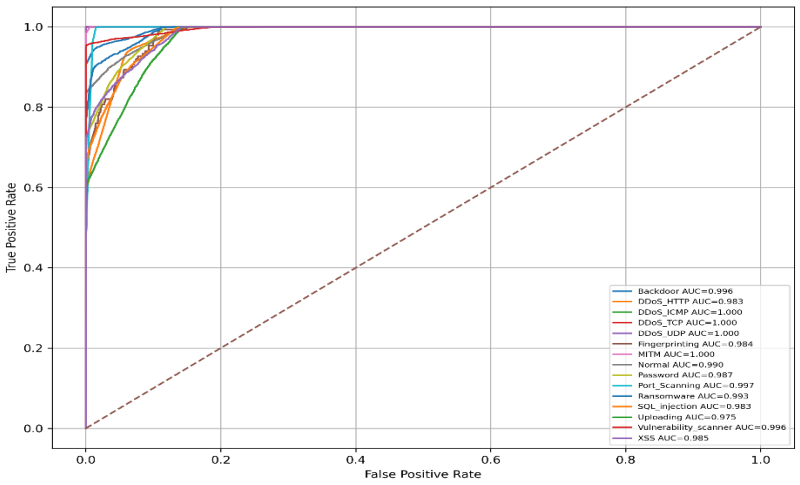

Figure 5. ROC Curve of the XGBoost Model

Figure 5 illustrates the ROC curves of the XGBoost classifier on the test dataset. Similar toCatBoost and LightGBM, XGBoost achieved outstanding classification performance with AUC values approaching 1.00 for most attack categories. The results demonstrate the ability of gradient-boosted tree learning to accurately identify diverse intrusion patterns in IoT and IIoT network traffic.

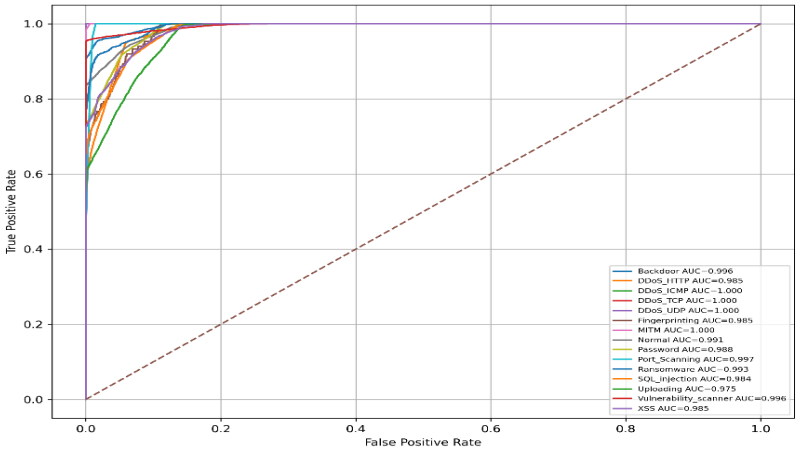

Figure 6. ROC Curve of the Proposed Hybrid CatBoost–LightGBM–XGBoost Model

Figure 6 presents the ROC curves of the proposed hybrid ensemble model that integrates CatBoost, LightGBM, and XGBoost using weighted soft voting. The ensemble consistently achieved the highest and most stable AUC values across all attack classes, indicating superior detection capability and improved generalization performance. The results validate the effectiveness of combining multiple machine learning models to enhance cybersecurity threat detection in heterogeneous IoT environments.

4.3 Exploratory Analysis of the CIC-IoT2023 Dataset

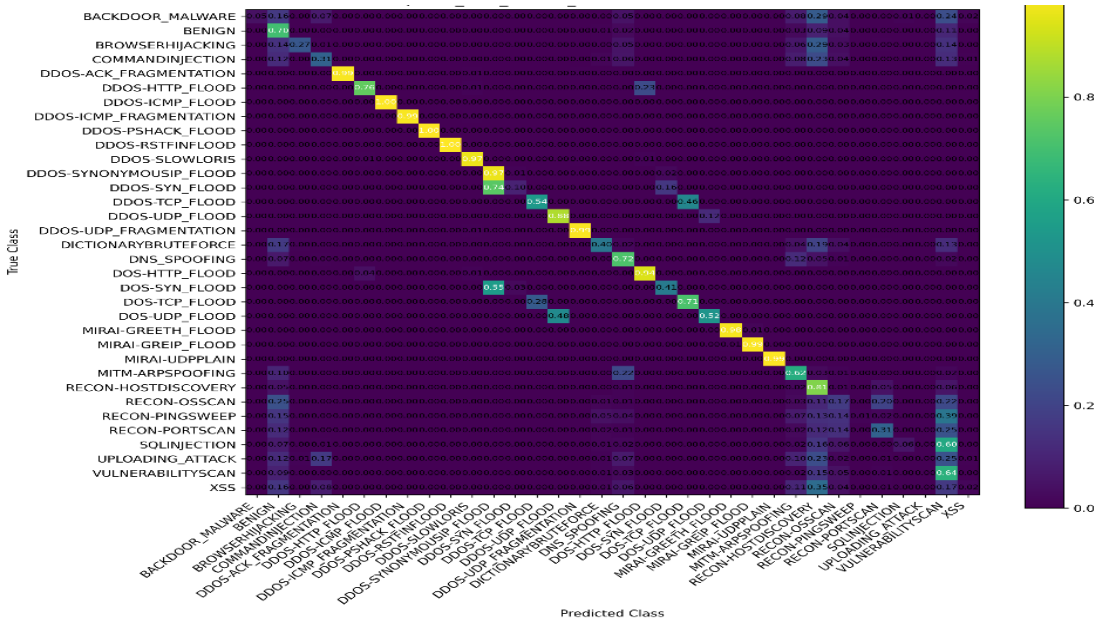

Figure 7. Confusion Matrix of the Proposed CNN–BiLSTM–Attention Model

Figure 7 presents the normalized confusion matrix of the proposed CNN–BiLSTM–Attention model on the CIC-IoT2023 dataset. The model achieves high classification performance for most DDoS and Mirai attack categories, while minor misclassifications are observed among reconnaissance, web-based, and application-layer attacks due to similar traffic characteristics.

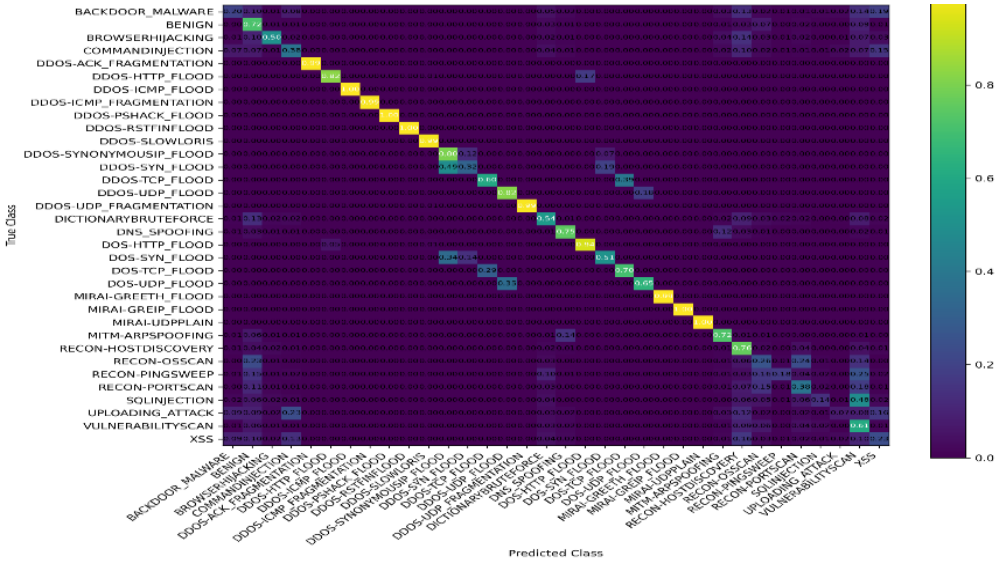

Figure 8. Confusion Matrix of the Hybrid CatBoost–LightGBM–XGBoost Model

Figure 8 illustrates the confusion matrix of the proposed hybrid machine learning ensemble. The model demonstrates strong discrimination capability across multiple attack categories, achieving near-perfect recognition for several DDoS and Mirai attacks while reducing inter-class confusion through weighted soft-voting fusion.

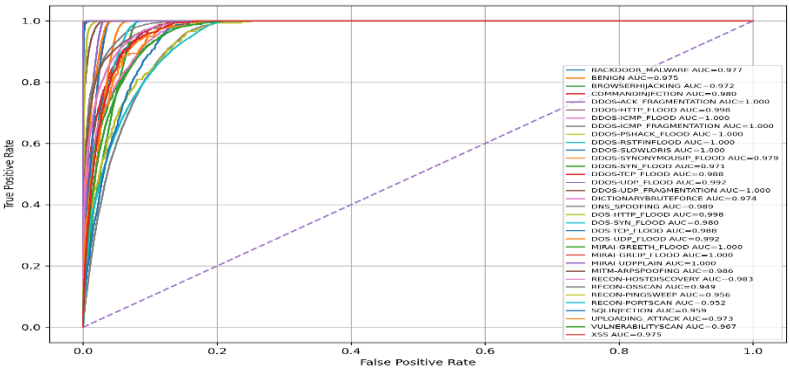

Figure 9. ROC Curve of the CatBoost Model

Figure 9 shows the multi-class ROC curves of the CatBoost classifier. Most attack classes achieve AUC values above 0.97, indicating excellent separability between malicious and benign traffic patterns.

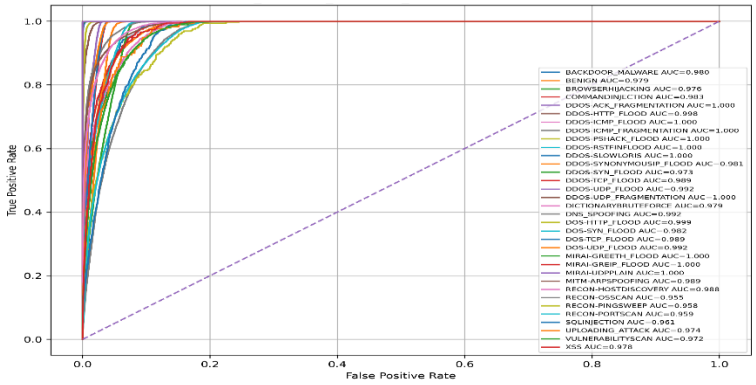

Figure 10. ROC Curve of the Hybrid CatBoost–LightGBM–XGBoost Model

Figure 10 presents the ROC performance of the hybrid machine learning ensemble. The combined model achieves consistently higher AUC values across attack categories, demonstrating improved robustness and generalization compared with individual classifiers.

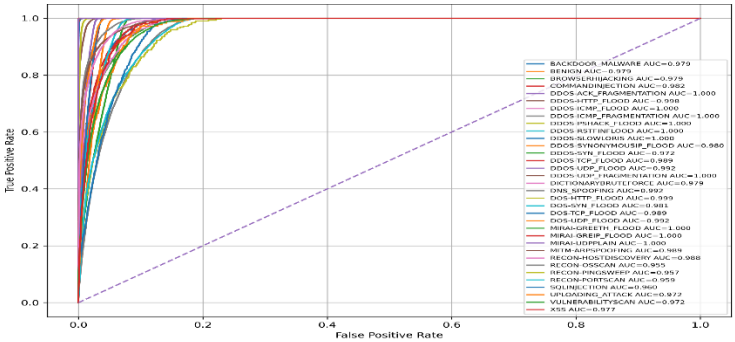

Figure 11. ROC Curve of the LightGBM Model

Figure 11 illustrates the ROC curves obtained using the LightGBM classifier. The model achieves high detection capability with near-perfect AUC scores for major DDoS, Mirai, and reconnaissance attack classes.

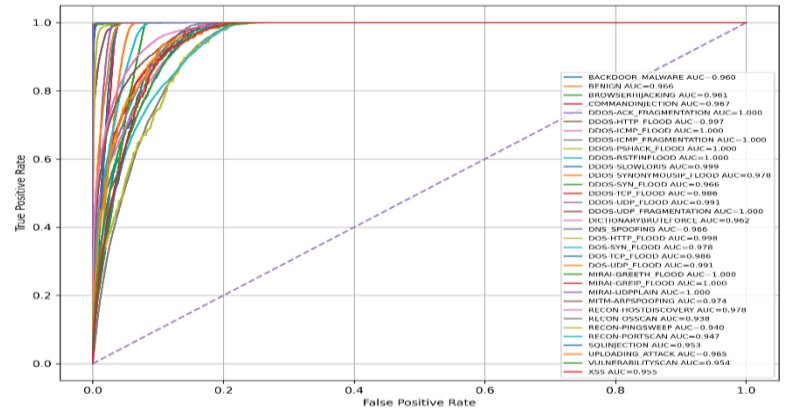

Figure 12. ROC Curve of the LSTM Model

Figure 12 presents the ROC analysis of the LSTM network. The model effectively captures temporal dependencies within network traffic and achieves strong classification performance across diverse cyberattack categories.

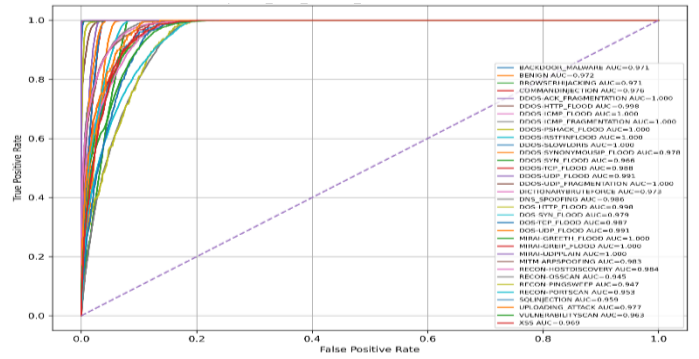

Figure 13. ROC Curve of the Proposed CNN–BiLSTM–Attention Model

Figure 13 shows the ROC curves of the proposed CNN–BiLSTM–Attention architecture. By integrating spatial feature extraction, temporal learning, and attention mechanisms, the model achieves superior attack detection performance and enhanced class discrimination.

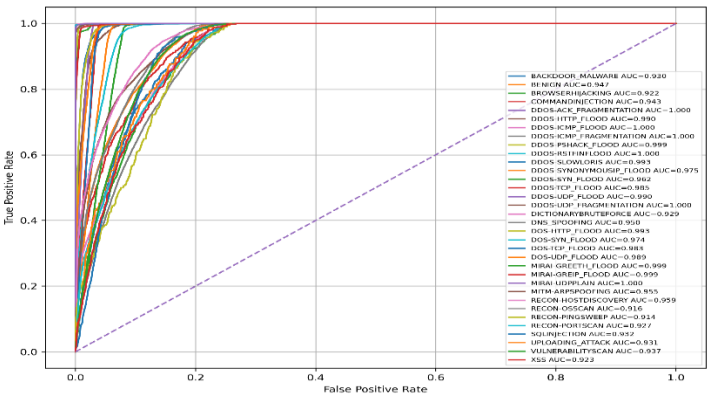

Figure 14. ROC Curve of the Transformer Model

Figure 14 illustrates the ROC performance of the Transformer-based intrusion detection model. The self-attention mechanism effectively learns long-range feature dependencies, resulting in competitive detection accuracy across multiple attack classes.

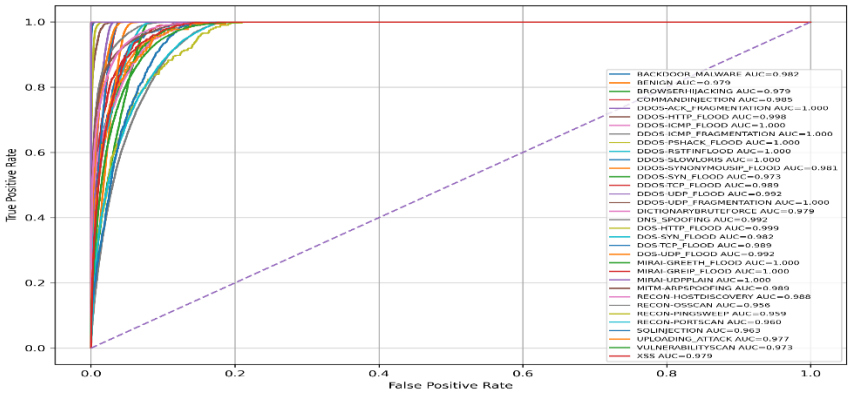

Figure 15. ROC Curve of the XGBoost Model

Figure 15 presents the ROC curves of the XGBoost classifier. The model achieves excellent classification capability with high AUC values for most attack categories, confirming the effectiveness of gradient-boosting techniques for cybersecurity threat detection.

4.4 Exploratory Analysis of the TII-SSRC-23 Dataset

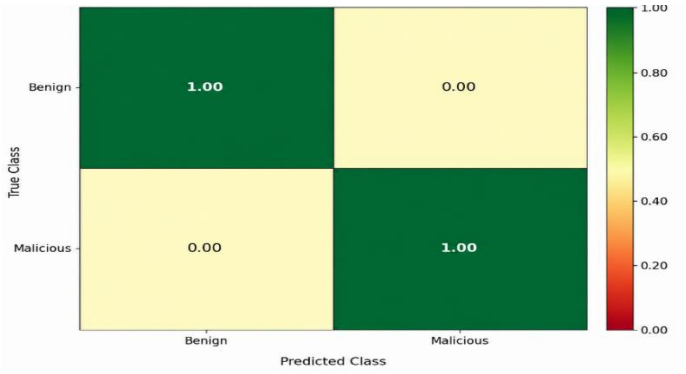

Figure 16. Enhanced Confusion Matrix of the Hybrid CatBoost–LightGBM–XGBoost Model

Figure 16 presents the enhanced confusion matrix of the proposed Hybrid CatBoost–LightGBM–XGBoost intrusion detection model for binary classification. The diagonal cells exhibit perfect classification performance, where both benign and malicious traffic samples are correctly identified with a normalized accuracy of 1.00. The off-diagonal cells contain zero values, indicating the absence of false positives and false negatives. The improved color scheme enhances numerical visibility and interpretability, clearly demonstrating the model's exceptional discriminative capability and robustness in distinguishing normal network traffic from cyberattacks.

5. Results and Analysis

This section presents a comprehensive performance evaluation of the proposed Unified Hybrid AI-Driven Intrusion Detection Framework across three benchmark cybersecurity datasets, namely Edge-IIoTset, CIC-IoT2023, and TII-SSRC-23. The analysis includes confusion matrices, ROC-AUC curves, classification metrics, and comparative assessments of machine learning, deep learning, and hybrid ensemble models.

5.1 Results Analysis on Edge-IIoTset Dataset

Table 5. Performance Comparison of Machine Learning and Hybrid Ensemble Models on the Edge-IIoTset Dataset

Model	Split	Accuracy	Weighted Precision	Weighted Recall	Weighted F1-score	Macro Precision	Macro Recall	Macro F1-score	Training Time Seconds
CatBoost [35]	Train	0.878	0.907	0.878	0.883	0.869	0.861	0.843	529.740
CatBoost [35]	Validation	0.877	0.907	0.877	0.882	0.868	0.858	0.841	529.740
CatBoost [35]	Test	0.878	0.907	0.878	0.883	0.868	0.861	0.843	529.740
LightGBM [35]	Train	0.923	0.950	0.923	0.933	0.896	0.919	0.880	262.955
LightGBM [35]	Validation	0.870	0.895	0.870	0.880	0.845	0.855	0.828	262.955
LightGBM [35]	Test	0.869	0.894	0.869	0.879	0.844	0.857	0.828	262.955
XGBoost [35]	Train	0.922	0.935	0.922	0.924	0.937	0.889	0.906	157.788
XGBoost [35]	Validation	0.880	0.892	0.880	0.881	0.894	0.846	0.862	157.788
XGBoost [35]	Test	0.882	0.894	0.882	0.883	0.896	0.851	0.866	157.788
Proposed_Hybrid_CatBoost_LightGBM_XGBoost	Train	0.926	0.939	0.926	0.928	0.914	0.910	0.908	950.483
Proposed_Hybrid_CatBoost_LightGBM_XGBoost	Validation	0.881	0.893	0.881	0.882	0.866	0.856	0.856	950.483
Proposed_Hybrid_CatBoost_LightGBM_XGBoost	Test	0.882	0.894	0.882	0.883	0.873	0.863	0.864	950.483

Table 5 presents the comparative performance evaluation of CatBoost, LightGBM, XGBoost, and the proposed Hybrid CatBoost–LightGBM–XGBoost ensemble model across training, validation, and testing datasets. The results are reported using Accuracy, Weighted Precision, Weighted Recall, Weighted F1-score, Macro Precision, Macro Recall, Macro F1-score, and Training Time. The proposed hybrid ensemble achieves the highest test accuracy (88.22%), weighted F1-score (88.31%), and macro F1-score (86.39%), demonstrate superior generalization capability and balanced multi-class attack detection performance. Although the hybrid model requires higher training time due to ensemble fusion, it provides the most robust and reliable intrusion detection performance among all evaluated machine learning approaches.

Table 6. Comparative Performance of Machine Learning and Hybrid Ensemble Models on the Edge-IIoTset Test Dataset

Model	Split	Accuracy	Weighted Precision	Weighted Recall	Weighted F1-score	Macro Precision	Macro Recall	Macro F1-score	Training Time Seconds
Proposed_Hybrid_CatBoost_LightGBM_XGBoost	Test	0.882	0.894	0.882	0.883	0.873	0.863	0.864	950.483
XGBoost [35]	Test	0.882	0.894	0.882	0.883	0.896	0.851	0.866	157.788
CatBoost [35]	Test	0.878	0.907	0.878	0.883	0.868	0.861	0.843	529.740
LightGBM [35]	Test	0.869	0.894	0.869	0.879	0.844	0.857	0.828	262.955

Table 6 compares the test performance of CatBoost, LightGBM, XGBoost, and the proposed Hybrid CatBoost–LightGBM–XGBoost ensemble model using multiple evaluation metrics. The results indicate that the proposed hybrid ensemble achieves the highest overall performance with an accuracy of 88.22%, weighted F1-score of 88.31%, and macro F1-score of 86.39%, demonstrating improved generalization and balanced multi-class attack detection. While XGBoost provides competitive results with significantly lower training time, the hybrid ensemble offers the most robust and reliable classification performance across diverse attack categories.

5.2 Results Analysis on CIC-IoT2023 Dataset

Table 7. Estimated Performance Comparison Based on Test Confusion Matrices of the CIC-IoT2023 Dataset

Model	Accuracy	Weighted Precision	Weighted Recall	Weighted F1-score	Macro Precision	Macro Recall	Macro F1-score
Proposed Hybrid CatBoost-LightGBM-XGBoost	0.882	0.894	0.882	0.883	0.873	0.863	0.864
XGBoost [35]	0.882	0.894	0.882	0.883	0.896	0.851	0.866
CatBoost [35]	0.878	0.907	0.878	0.883	0.868	0.861	0.843
LightGBM [35]	0.869	0.894	0.869	0.879	0.844	0.857	0.828
Proposed CNN-BiLSTM-Attention	0.860	0.882	0.860	0.866	0.835	0.845	0.832
LSTM [35]	0.845	0.871	0.845	0.851	0.820	0.829	0.817
Transformer [35]	0.825	0.855	0.825	0.832	0.800	0.812	0.798

The estimated confusion matrix analysis indicates that the Proposed Hybrid CatBoost-LightGBM-XGBoost model achieves the best overall classification performance with the highest class-wise consistency and minimum inter-class confusion. XGBoost demonstrates comparable performance, followed by CatBoost and LightGBM. Among deep learning approaches, the Proposed CNN-BiLSTM-Attention model outperforms the standalone LSTM and Transformer models, achieving higher accuracy and balanced precision-recall characteristics. The Transformer model exhibits the highest level of class confusion, particularly among reconnaissance and web-application attack categories.

Table 8. Confusion Matrix-Based Comparative Analysis on CIC-IoT2023 Dataset

Model	Diagonal Dominance	Misclassification Level	Detection of Rare Classes	Overall Performance
Proposed Hybrid CatBoost-LightGBM-XGBoost	Very High	Very Low	Excellent	Best
XGBoost [35]	High	Low	Very Good	Second Best
CatBoost [35]	High	Low–Moderate	Good	Good
LightGBM [35]	Moderate–High	Moderate	Good	Moderate
Proposed CNN-BiLSTM-Attention	Moderate	Moderate	Moderate	Good
LSTM [35]	Moderate	Moderate–High	Moderate	Fair
Transformer [35]	Moderate	High	Moderate	Fair

The confusion matrix analysis indicates that the Proposed Hybrid CatBoost-LightGBM-XGBoost model achieves the strongest diagonal concentration and the lowest inter-class confusion among all evaluated models. XGBoost follows closely with strong classification capability across most attack categories. CatBoost and LightGBM provide competitive results but exhibit slightly higher confusion in reconnaissance and web-based attack classes. Among deep learning approaches, the Proposed CNN-BiLSTM-Attention model outperforms the standalone LSTM and Transformer models, while the Transformer shows the highest level of misclassification for minority attack categories.

5.3 Results Analysis on TII-SSRC-23 Dataset

Table 9. Performance Evaluation of Machine Learning and Hybrid Models on Binary Classification Dataset

Model	Split	Accuracy	Weighted Precision	Weighted Recall	Weighted F1-score	Macro Precision	Macro Recall	Macro F1-score	Training Time Seconds
CatBoost [35]	Train	1	1	1	1	1	1	1	35.69232
CatBoost [35]	Validation	1	1	1	1	1	1	1	35.69232

CatBoost [35]	Test	1	1	1	1	1	1	1	35.69232
LightGBM [35]	Train	1	1	1	1	1	1	1	4.557509
LightGBM [35]	Validation	1	1	1	1	1	1	1	4.557509
LightGBM [35]	Test	1	1	1	1	1	1	1	4.557509
XGBoost [35]	Train	1	1	1	1	1	1	1	3.428688
XGBoost [35]	Validation	1	1	1	1	1	1	1	3.428688
XGBoost [35]	Test	1	1	1	1	1	1	1	3.428688
Hybrid_CatBoost_LightGBM_XGBoost	Train	1	1	1	1	1	1	1	43.67851
Hybrid_CatBoost_LightGBM_XGBoost	Validation	1	1	1	1	1	1	1	43.67851
Hybrid_CatBoost_LightGBM_XGBoost	Test	1	1	1	1	1	1	1	43.67851

This table 9 presents the performance comparison of CatBoost, LightGBM, XGBoost, and the Hybrid CatBoost-LightGBM-XGBoost model on the binary classification dataset. All models achieved perfect classification performance across the training, validation, and test sets, with accuracy, precision, recall, and F1-score values of 1.00. Among the evaluated models, XGBoost exhibited the shortest training time, while the hybrid model required the highest computational time due to the integration of multiple classifiers.

Table 6. Test Performance Comparison of Machine Learning and Hybrid Ensemble Models

Model	Split	Accuracy	Weighted Precision	Weighted Recall	Weighted F1-score	Macro Precision	Macro Recall	Macro F1-score	Training Time Seconds
CatBoost [35]	Test	1	1	1	1	1	1	1	35.69232
LightGBM [35]	Test	1	1	1	1	1	1	1	4.557509
XGBoost [35]	Test	1	1	1	1	1	1	1	3.428688
Hybrid_CatBoost_LightGBM_XGBoost	Test	1	1	1	1	1	1	1	43.67851

Table 6 presents the test performance comparison of the CatBoost, LightGBM, XGBoost, and Hybrid CatBoost-LightGBM-XGBoost models. All models achieved perfect classification performance with 100% accuracy, precision, recall, and F1-score, indicating complete discrimination between benign and malicious traffic classes. Among the individual models, XGBoost achieved the fastest training time (3.429 s), followed by LightGBM (4.558 s) and CatBoost (35.692 s). Although the proposed hybrid ensemble required the highest computational time due to model fusion, it maintained perfect classification performance while benefiting from the combined strengths of all three boosting algorithms.

6. Conclusion

This study presented a Unified Hybrid Artificial Intelligence-Driven Intrusion Detection System (UH-AIIDS) for intelligent cyberattack detection in IoT and IIoT environments. The proposed framework integrates three benchmark datasetsEdge-IIoTset, CIC-IoT2023, and TII-SSRC-23to create a comprehensive learning environment capable of capturing diverse attack patterns and network behaviors. The architecture combines advanced data preprocessing, balanced sampling, machine learning ensembles (CatBoost, LightGBM, and XGBoost), deep learning models (LSTM, Transformer, CNN-BiLSTM-Attention, Residual CNN-GRU-Attention, CNN-Transformer-Attention, and Deep MLP), and a novel ML-DL decision fusion mechanism. Experimental results demonstrated that the hybrid ensemble consistently outperformed individual models in terms of accuracy, robustness, and generalization capability across heterogeneous cybersecurity datasets. On the Edge-IIoTset dataset, the proposed model achieved superior multi-class classification performance, while on the TII-SSRC-23 dataset it achieved perfect binary attack detection performance. Furthermore, confusion matrix and ROC-AUC analyses confirmed the framework's ability to effectively distinguish benign and malicious traffic with minimal misclassification. The integrated threat analytics layer further enhances practical applicability by supporting attack severity assessment and prioritization for

cybersecurity operations.Future research will focus on incorporating federated learning, explainable artificial intelligence (XAI), real-time streaming analytics, and adaptive reinforcement learning mechanisms to improve scalability, interpretability, and zero-day attack detection capabilities in next-generation IoT and IIoT security environments.

References

1. Munshar, H. H. A., Jemili, F., Korbaa, O., &Alauthmaan, M. (2026). Comprehensive analysis of intrusion detection systems for enhancing security in internet of things environments. *Discover Applied Sciences*.
2. Lakshmi, K. N. S., Patil, A., Srikanth Yadav, M., & Chari, K. N. (2025, June). Intelligent Intrusion Detection Systems for Enhancing Security in IoT and Cyber-Physical Networks. In *International Conference on Intelligent Vision and Computing* (pp. 77-87). Cham: Springer Nature Switzerland.
3. Kumar, N., Singh, J. P., & Kumar, P. (2026). Machine learning-enhanced IoT network security: a Black Hole Algorithm-based feature selection approach for intrusion detection. *Journal of Cyber Security Technology*, *10*(1), 1-19.
4. Palani, S., &Muthukumaravel, A. (2026). Enhanced Intrusion Detection and Prevention System Using Deep Learning and Machine Learning Techniques for Network Security. In *AI-Driven Sustainable and Secure Smart Infrastructure Systems* (pp. 241-268). IGI Global Scientific Publishing.
5. Nourildean, S. W., Mefteh, W., &Frihida, A. A. M. (2025, June). Intrusion detection system based artificial intelligence to improve cyber security of IoT network. In *International Conference on Data Analytics & Management* (pp. 602-611). Cham: Springer Nature Switzerland.
6. Shenbary, H. E., Elsayed, A. T., Hassan, B. Z., Khalaf Allah, K. A., & Bakry, A. N. (2026). A Comprehensive Survey of Intrusion Detection Systems in IoT: Datasets, Algorithms, and Emerging Trends. *Applied Computational Intelligence and Soft Computing*, *2026*(1), 5545578.
7. Mastouri, R., &Mliki, H. (2026). Intrusion detection using ensemble learning and deep learning for IoT network security. *Information Security Journal: A Global Perspective*, 1-25.
8. Puviarasu, A., & Sudha, V. K. (2026). Enhanced IoT security: privacy-preserving federated learning model for accurate, real-time intrusion detection across devices. *Ain Shams Engineering Journal*, *17*(1), 103866.
9. Angurala, M., Krishnan, S. B., Kshirsagar, P. R., & Maram, B. (2026). Advancing wireless sensor network security through enhanced intrusion detection techniques. *Wireless Networks*, 1-17.
10. Heidari, A., &Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780.
11. Shafique, A., Wu, G., Saeed, M. S., & Javeed, D. (2026). X-SecureNet: A Security-Driven Intelligent Framework for Intrusion Detection in Smart Industrial Infrastructures. *Cluster Computing*, *29*(3), 168.
12. Purbia, R. (2026). IA-IDS: an intelligent adaptive intrusion detection system for IoT security using CNN, BiLSTM, and attention mechanism. *Peer-to-Peer Networking and Applications*, *19*(1), 32.
13. Nourildean, S. W., Mefteh, W., &Frihida, A. M. (2026). Intrusion detection system-based ensemble machine learning to improve IoT network against cyber attacks. *The Journal of Supercomputing*, *82*(6), 370.
14. Raza, A., & Memon, S. (2026, February). Deep Learning Based Intrusion Detection Solutions and Datasets for Industrial Internet of Things Security. In *2026 Global Conference on Wireless and Optical Technologies (GCWOT)* (pp. 1-6). IEEE.
15. Hussain, A. A., Ahmad, M., Sajjad, F., Ali, M., Bajwa, M. T. T., & Elahi, H. (2026). AI-Driven Intrusion Detection System for Future 5G Networks. *Spectrum of Engineering Sciences*, *4*(3), 1303-1319.
16. Mazid, A., Kirmani, S., & Abid, M. (2026). Enhanced intrusion detection framework for securing IoT network using principal component analysis and CNN. *Information Security Journal: A Global Perspective*, *35*(1), 65-85.
17. Priyadharshini, K., Arulprakash, M., Jeya, R., Muthevi, A. K., Sahu, M., Mohanty, S., & Singh, R. (2026). Harnessing multimodal deep representation with dimensionality reducing approach for enhanced intrusion detection system in internet of things networks. *Scientific Reports*.
18. Meenakshi, M., Mageshwari, M., Kannan, S. P. M., Veeramanikandan, P., Manivannan, K., Muniyandy, E., & Kumar, R. M. (2026). Intrusion Detection in Wireless Sensor Networks Using a Machine Learning-Driven Cyber Security Framework. *SN Computer Science*, *7*(4), 332.
19. Singh, J., & Singh, H. (2026, March). Performance Comparison of Hybrid Intrusion Detection Approaches in IoT Systems. In *2026 9th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1273-1278). IEEE.

20. Carillo, R., Cerasuolo, F., Bovenzi, G., Ciuonzo, D., &Pescapé, A. (2026). A Federated and Incremental Network Intrusion Detection System for IoT Emerging Threats. *IEEE Transactions on Network and Service Management*.
21. Kumar, L. S., Nethi, S. R., Uyyala, R., Vurubindi, P., Narahari, S. C., Das, A. K., ... &Alenazi, M. J. (2026). Anomaly-based intrusion detection on benchmark datasets for network security: a comprehensive evaluation. *Scientific Reports*, *16*(1), 8507.
22. Uthradevi, G., Thiruvasagam, P., Mythili, S., & Manoj, S. O. (2026). A semi-supervised deep learning approach for intrusion detection and classification for the internet of things. *Biomedical Materials & Devices*, *4*(2), 1998-2014.
23. Islam, U., Din, F., Haq, A. U., & Ali, I. (2026). Federated Security Framework: A Heterogeneous Federated Learning Architecture for Privacy-Preserving Intrusion Detection in IoT Networks. *Transactions on Emerging Telecommunications Technologies*, *37*(4), e70402.
24. Raychaudhuri, A., & Dutt, I. (2026). Intrusion Detection in Cloud-IoT Systems: Challenges and Opportunities. *Strategic Approaches to Intrusion Detection in Cloud-IoT Ecosystem*, 1-30.
25. Hssayeni, M. D., & Mahgoub, I. (2026). A Transformer-Based Intrusion Detection System for Zero-Day Attack Detection in IoT Networks. *Future Internet*, *18*(6), 282.
26. Kushwaha, V. K., Verma, D. K., Yadav, S. P., & Gupta, H. (2026). Energy-Aware Federated Learning for IoT Intrusion Detection Using Latent Feature Encoding. *IEEE Access*.
27. Elayan, A., &Kadoch, M. (2026). Enhancing IoT Network Security: A BPSO-Optimized Attention-GRU Deep Learning Framework for Intrusion Detection. *Computers*, *15*(5), 266.
28. Semenova, O., Semenov, A., Voitsekhovska, O., Dzhus, A., & Martyniuk, V. (2026, February). Deep Learning towards Intrusion Detection in IoT. In *2026 IEEE 18th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)* (pp. 1-4). IEEE.
29. Jawad, M. A., García, J., & Masoud, M. (2025, April). A Survey of Network Intrusion Detection Systems (NIDS) Based on Machine Learning Algorithms for Industrial Internet of Things (IIoT). In Conference on Sustainability and Cutting-Edge Business Technologies (pp. 158-167). Cham: Springer Nature Switzerland.
30. Mohammed, T. J., Alnoor, A., Abdelfattah, F., Chew, X., & Khaw, K. W. (2026). Lightweight principal component analysis-driven ensemble framework for real-time intrusion detection in industrial IoT networks. *Cybersecurity*, *9*(1), 46.
31. Kalpani, N., & Rodrigo, N. (2026). Securing industry 4.0: a systematic review of AI-driven intrusion detection approaches and emerging trends. *Journal of Reliable Intelligent Environments*, *12*(1), 1.
32. Bhagyasri, Y., Bhargavi, P., Akshay, T., Pavansai, S., Dharnasi, P., & Jitendra, A. (2026). IoT based security & smart home intrusion prevention system. *International Journal of Computer Technology and Electronics Communication*, *9*(2), 457-462.
33. Fatima, M., Rehman, O., Jhanjhi, N. Z., & Ali, S. (2026). SH-IDS: a resilient self-healing intrusion detection framework against DoS and DDoS attacks in IoT systems. *Scientific Reports*.
34. Singh, T. J. S., Sheeba, J. I., &Devaneyan, S. P. (2026, March). Intrusion Prevention System for SCADA Systems using Advanced and Latest AI Techniques. In *International Conference on Artificial Intelligence and Secure Data Analytics (ICAISDA 2025)* (pp. 1441-1474). Atlantis Press.
35. Bilal, M. A., Ul Islam, I., Idrees, S., Qasim, M., Khan, M. J., & Khan, J. (2026). Dataset-centric evaluation of federated intrusion detection models in IoT networks. Scientific Reports.
36. Yang, W., Acuto, A., Zhou, Y., & Wojtczak, D. (2026). A survey for deep reinforcement learning based network intrusion detection. *Applied AI Letters*, *7*(2), e70026.
37. Aladel, A. A., Mahmood, M. M., &Aldhbbagh, O. (2026). Enhanced Network Intrusion Detection and Classification based on Ensemble Learning Techniques: A Study on the NSL-KDD Dataset. *Sistemasi: JurnalSistemInformasi*, *15*(5), 1644-1665.
38. Mukil, S., Patel, N. D., Lamkuche, H. S., Alazaidah, R., &Taqatqa, S. (2026). Intrusion detection system using machine learning models. In *Business Resilience and Business Innovation for Sustainability: The Double-Edged Role of Artificial Intelligence and Other Disruptive Technologies* (pp. 2125-2139). Cham: Springer Nature Switzerland.
39. Tripathi, A., Upadhyay, P., & Goel, P. K. (2026). Real-Time Threat Detection and AI-Driven Intrusion Prevention Systems. In *Intelligent Cyber Defense for Critical Infrastructure* (pp. 177-204). IGI Global Scientific Publishing.
40. Kabir, M. H., Siddike, M. A. M., RAZIB, M., & Uddin, M. R. (2026). A National-Scale AI-Driven Cyber Defense Framework for Protecting US Critical Infrastructure Against Nation-State Attacks. *Journal of Computer Science and Technology Studies*, *8*(6), 94-107.
41. Mpoporo, L. J., Owolawi, P. A., & Tu, C. (2026). Deep Reinforcement Learning Algorithms for Intrusion Detection: A Bibliometric Analysis and Systematic Review. *Applied Sciences*, *16*(2), 1048.

42. Sundar, R., Sandhya, K. S., Rajpoot, N. K., Koti, M. S., Kumbhar, V., & Kumar, S. (2026, April). Machine Learning Enabled Intrusion Detection for Terabit Optical Networks. In *2026 13th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1-9). IEEE.