Cureus Journal of Computer Science

Open Access Case Study

Dynamic Neuro-Fuzzy Vulnerability Detection System (DNF-VDS)

Kavita U. Rahane [1] , Anil B. Pawar [1]

1. Computer Engineering, Sanjivani College of Engineering, Savitribai Phule Pune University, Kopargaon, IND

Corresponding author: Kavita U. Rahane, rahane_kavita@yahoo.co.in

Received 07/01/2025
Review began 08/07/2025
Review ended 12/22/2025
Published 01/12/2026

DOI:
https://doi.org/10.7759/s44389-025-00009-3

Abstract

The rapid expansion of Industrial Internet of Things (IIoT) infrastructures has introduced a complex, heterogeneous ecosystem that is increasingly vulnerable to diverse cyberattacks. Traditional machine learning- and deep learning-based intrusion detection systems provide strong predictive performance but lack interpretability, rely on static models, and fail to adapt to evolving attack patterns. This study proposes a Dynamic Neuro-Fuzzy Vulnerability Detection System (DNF-VDS) that integrates fuzzy rule-based reasoning with neural network-driven parameter optimization. The system supports automatic rule generation, continuous rule updating, and membership function adaptation, enabling interpretable and adaptive vulnerability detection suited for dynamic IIoT environments.

Using the Edge-IIoTset dataset, the proposed system achieves 95% accuracy, 93.5% F1-score, and a false positive rate of 5%, outperforming baseline models, including Bidirectional Long Short-Term Memory, Support Vector Machine, Random Forest, and Decision Tree. Statistical significance testing confirms that improvements are non-random ($p < 0.05$). Unlike prior neuro-fuzzy approaches, DNF-VDS demonstrates quantifiable interpretability through rule analysis and activation profiling while maintaining scalability for industrial deployment. These findings establish DNF-VDS as a transparent, adaptive, and high-performing solution for IIoT vulnerability detection. Future work will explore real-time deployment and distributed learning across industrial nodes.

Categories: Fuzzy Logic, Security and Privacy, IoT Security and Privacy
Keywords: internet of things, machine learning, deep learning, neural network, fuzzy logic

Introduction

The rapid expansion of Industrial Internet of Things (IIoT) ecosystems across manufacturing, healthcare, energy, and transportation has increased the scale and complexity of cyber-physical infrastructures [1,2]. While IIoT enables automation and real-time analytics, it simultaneously exposes these systems to evolving vulnerabilities, resource constraints, and heterogeneous communication frameworks [3]. Conventional intrusion detection and vulnerability detection approaches - such as signature-based intrusion detection systems (IDS) or static rule-based systems - struggle to handle IIoT's noisy, high-velocity, and non-stationary data streams [4].

Machine learning (ML) and deep learning (DL) have emerged as promising techniques for anomaly detection in IIoT environments [5-7]. However, ML/DL models often lack interpretability and require expensive retraining when network behavior shifts, limiting their suitability for real-time industrial monitoring [8]. Deep models, although effective at learning complex patterns, act as black boxes and often fail to satisfy explainability and transparency requirements in safety-critical domains [9].

Neuro-fuzzy systems aim to bridge the gap between interpretability and adaptability by integrating fuzzy rule-based reasoning with neural learning [10]. Prior studies demonstrate their ability to manage uncertainty in cybersecurity data, but most neuro-fuzzy IDS implementations suffer from static rule bases, fixed membership functions (MFs), limited dataset evaluation, and shallow integration with ML/DL pipelines [11-13]. The absence of dynamic rule-adaptation mechanisms reduces resilience to concept drift and evolving attack strategies.

To address these limitations, this work proposes the Dynamic Neuro-Fuzzy Vulnerability Detection System (DNF-VDS) - a hybrid adaptive framework combining fuzzy interpretability, neural learning, dynamic rule updating, and ML/DL fusion. DNF-VDS introduces:

1. A Dynamic Rule Updating Mechanism (DRUM) that adapts its rule base and MFs in real time;

2. A hybrid inference pipeline integrating neuro-fuzzy reasoning with ML/DL models;

3. Transparent, human-readable rules suitable for industrial auditability;

How to cite this article
Rahane K U, Pawar A B (January 12, 2026) Dynamic Neuro-Fuzzy Vulnerability Detection System (DNF-VDS). Cureus J Comput Sci 3 : es44389-025-00009-3. DOI https://doi.org/10.7759/s44389-025-00009-3

4. Rigorous evaluation using the Edge-IIoT dataset [14].

This contribution advances current cybersecurity research by delivering an IIoT-specific detection framework that is adaptive to concept drift, interpretable to operators, and validated through detailed empirical analysis. The following manuscript sections present the challenges in smart vulnerability detection, a comprehensive literature review, the proposed neuro-fuzzy methodology, experimental evaluation, and the system's real-world applicability.

Challenges in vulnerability detection in smart systems

Modern IIoT and smart computing environments present a unique set of challenges for designing effective and adaptive vulnerability detection systems. These environments operate across distributed, heterogeneous devices with diverse operating systems, communication protocols, and hardware capabilities. The following subsections summarize the key challenges that motivate the development of adaptive and interpretable detection frameworks such as DNF-VDS.

Device Heterogeneity

IIoT infrastructures integrate sensors, controllers, embedded devices, and industrial nodes operating across varied architectures and protocols. This heterogeneity results in widely differing traffic patterns, packet structures, and resource capabilities. Static or protocol-specific vulnerability detection methods often fail to generalize across such diverse device behaviors. Furthermore, inconsistencies in vendor implementations increase the likelihood of misconfigurations that create additional attack vectors [15,16].

Expanded Cyber-Physical Attack Surface

The large-scale interconnection of IIoT devices expands the potential attack surface dramatically. Each device becomes a potential point of compromise, and an outdated or misconfigured component can jeopardize the entire network. Modern adversaries exploit this landscape using advanced multi-stage campaigns, lateral movement, botnet propagation (e.g., Mirai-like malware), and low-footprint reconnaissance techniques that bypass signature-based detection [17,18].

Real-Time Processing Requirements

Industrial control systems and smart manufacturing processes require ultra-low-latency detection to ensure operational continuity and safety. Existing ML/DL models often incur high inference costs and require substantial computational resources, making them unsuitable for edge-deployed IIoT environments [19]. Lightweight yet accurate detection mechanisms are crucial.

Limited Computational and Memory Resources

Many IIoT devices operate with restricted CPU capabilities, small memory footprints, and limited power availability. These devices cannot support computationally heavy or frequently retrained ML/DL models [20]. As a result, traditional IDS solutions - especially deep architectures - struggle to deliver real-time, edge-compatible detection.

Legacy Systems and Outdated Firmware

Industrial deployments often incorporate legacy devices with outdated firmware that cannot be patched or updated frequently. These devices lack modern security primitives, increasing susceptibility to privilege escalation, remote code execution, and man-in-the-middle attacks [21]. The difficulty of patching firmware at scale necessitates proactive vulnerability detection mechanisms.

Noisy, Incomplete, and Non-Stationary Data

IIoT data streams are frequently noisy, incomplete, and affected by abrupt distribution shifts due to sensor malfunctions, environmental changes, dynamic workloads, firmware updates, and operational mode transitions. This non-stationarity, often referred to as concept drift, renders static or pre-trained models [22,23] inadequate. Adaptive systems must be able to continuously update rules, MFs, and decision boundaries.

Lack of Standardized Security Protocols

Varying levels of security compliance across vendors contribute to inconsistencies in authentication, data encryption, and network isolation [24]. These inconsistencies complicate security monitoring and make

attack detection protocols heavily context-dependent.

Advanced Persistent Threats (APTs)

Modern APT campaigns leverage stealthy, multi-stage infiltration strategies that evade anomaly signatures through prolonged reconnaissance, low-and-slow traffic patterns, adaptive evasion strategies, and targeted privilege escalation. Traditional IDS approaches - whether signature-based or non-adaptive ML models - struggle to detect evolving APT behaviors [25] without retraining or dynamic update mechanisms.

Human and Configurational Factors

Misconfigured access controls, weak passwords, inconsistent patching schedules, and inadequate cybersecurity training among operators introduce preventable vulnerabilities. These human factors persist across industrial environments and interact with technological weaknesses to produce complex attack surfaces.

Summary of Challenges

Collectively, these challenges highlight the need for a dynamic, adaptive, interpretable, and lightweight vulnerability detection framework capable of evolving with IIoT environments. This motivates the development of DNF-VDS, which integrates fuzzy interpretability with neural adaptation and ML/DL fusion to address heterogeneity, concept drift, and real-time inference constraints

Case Presentation

Literature review

Accurate and adaptive vulnerability detection in IIoT environments has attracted significant research attention in recent years. Existing approaches can be broadly categorized into traditional rule-based systems, ML-based methods, and DL architectures.

This section critically reviews the strengths and limitations of each category positioning the proposed DNF-VDS within the current state of research.

Rule-Based and Signature-Based Vulnerability Detection

Traditional IDSs predominantly depend on predefined signatures or manually crafted rule sets to identify known attacks, as widely adopted in systems such as Snort and Suricata [26,27]. While these signature-based approaches deliver high precision for well-documented threats, they struggle considerably when confronted with emerging, unknown, or zero-day vulnerabilities. Their limitations are further intensified within dynamic IIoT environments, where heterogeneous and continuously evolving traffic leads to increased false positives. Since rules do not automatically update to reflect new behaviors, human experts must manually curate signatures, introducing delays in response time. Moreover, static rule sets cannot cope with concept drift, reducing long-term reliability. Thus, although conventional rule-based IDS methods offer strong interpretability, their lack of adaptability makes them insufficient for securing modern IIoT systems.

ML-Based Vulnerability Detection

ML models have been widely applied for anomaly detection and vulnerability classification, including Support Vector Machines (SVM), Random Forest (RF), Decision Trees (DT), k-Nearest Neighbors (KNN), and Naive Bayes (NB). These models can detect previously unseen anomalies but suffer from several limitations:

•Black-box decision boundaries restrict interpretability.

• Retraining required when data distributions shift.

• High-dimensional IIoT features cause overfitting or high variance.

• Feature engineering complexity is high for large heterogeneous datasets.

• Non-stationary IIoT environments [28-30] often render static ML models inadequate without adaptive learning mechanisms.

DL Approaches

DL architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks, Gated Recurrent Units, and BiLSTMs [31-33] have demonstrated strong performance in network intrusion detection. Several works employ CNN-based feature extraction, Long Short-Term Memory/BiLSTM for temporal modelling, autoencoders for anomaly detection, and Generative Adversarial Networks for adversarial training and synthetic data generation. Although DL achieves high accuracy, key limitations persist:

• Poor interpretability makes decisions difficult to justify in industrial settings.

• High computational cost restricts deployment at edge devices.

• Large training sets required, which is a challenge for specialized IIoT deployments.

• Limited adaptability without complete retraining.

Thus, while powerful, DL approaches lack the transparency required for safety-critical IIoT environments.

Neuro-Fuzzy Systems for Security

Neuro-fuzzy frameworks combine fuzzy logic's explainability with neural networks' adaptive learning. Prior studies have explored Adaptive Neuro-Fuzzy Inference System (ANFIS) [34-36], Hybrid Fuzzy-Neural Networks Fuzzy clustering (e.g., subtractive clustering, FCM), and Fuzzy rule pruning and classification. Advantages include human-readable rules, ability to manage uncertainty, interpretation of decision paths, and integration of expert knowledge. However, existing neuro-fuzzy vulnerability detection systems suffer from:

• Static or fixed rule bases, lacking online updates.

• Inadequate MF adaptation, with many studies using fixed or manually tuned MFs.

• Limited IIoT-specific evaluation, often relying on outdated datasets.

• Weak integration with ML/DL pipelines, resulting in suboptimal performance.

• Insufficient documentation of rule derivation or inference procedures.

Thus, the current generation of neuro-fuzzy IDS frameworks does not fully meet IIoT's requirements for explainable adaptive detection.

Hybrid Learning Models

Hybrid models combining fuzzy logic [37-38] with ML/DL algorithms have shown promise by merging interpretability with robustness. Existing hybrid approaches include Fuzzy-CNN [39] models for traffic classification, Fuzzy-Long Short-Term Memory [40] systems for temporal anomaly detection, Ensemble ML models with fuzzy rule adjustment, and ANFIS [41] based classifiers with evolutionary optimization. While these models outperform standalone algorithms, key limitations remain:

• Absence of dynamic rule-learning mechanisms

• Limited attention to real-time adaptation

• No comprehensive evaluation under concept drift

• Computational inefficiency for edge deployment

• Lack of transparency in how fuzzy rules interact with learned features.

These constraints highlight the need for a hybrid adaptive framework suitable for IIoT environments.

Comparison With Existing Studies

Based on the findings from the reviewed literature, prior vulnerability detection approaches exhibit notable strengths but also significant shortcomings, particularly when applied to dynamic IIoT

environments, as shown in Table 1.

Sr. No.	Reference No.	Technique	Improvement/Key Insight	Accuracy/Performance
1. Neuro-Fuzzy Systems for Intrusion Detection				
1.	[42]	Neuro-Fuzzy Intrusion Detection System (NFIDS)	Combines fuzzy logic with neural networks to manage uncertainty in traffic data	Improved detection of complex patterns
2.	[43]	Ensemble of Neuro-Fuzzy Classifiers	Robust detection of DDoS attacks under uncertainty	High robustness claimed
3.	[44]	Adaptive Neuro-Fuzzy IDS	Adapts to evolving network behavior	Better adaptability and detection rate
4.	[45]	Neuro-Fuzzy vs Genetic-Fuzzy IDS	Comparative performance analysis	Hybrid improves accuracy & reduces false positives
5.	[46]	ANFIS for Internet Traffic IDS	Real-time threat detection	Enhanced reliability and adaptability
6.	[47]	Neuro-Fuzzy for Wireless Sensor Networks	IDS tailored for resource-constrained WSNs	High detection accuracy
7.	[48]	Neuro-Fuzzy Vulnerability Evaluation Framework	Evaluates resilience and accuracy of vulnerability models	High accuracy with criteria-based assessment
2. Adaptive Neuro-Fuzzy Inference Systems (ANFIS)				
8.	[49]	ANFIS for Portscan Detection	Compares with Fuzzy Inference & NN	Superior detection of scan behavior
9.	[50]	ANFIS for Malware Detection	Targets classification accuracy	Better precision in malware types
10.	[51]	ANFIS in Smart Grid Security	Detects cyber intrusions in smart grid environments	Real-time and contextual analysis
11.	[52]	ANFIS + Fuzzy C-Means	Detects SQL injection attacks	Accurate attack pattern recognition
3. Machine Learning (ML) and Deep Learning (DL) in Vulnerability Detection				
12.	[53]	Deep Learning Benchmark for Vulnerable Code	Proposes DL-based detection benchmark	Sets performance standards
13.	[54]	CodeBERT Embedding for Vulnerability Detection	Embedding-based vulnerability learning	Basis for optimized future models
14.	[55]	Survey on ML/DL in Vulnerability Detection	Reviews current methods, challenges, data issues	Emphasis on architecture robustness
15.	[56]	Learning-Based Model Study	Focuses on stability and interpretability	Encourages interpretable models
16.	[57]	Graph vs. Sequence-based DL Models	Comparative accuracy evaluation	Selection based on specific use cases
4. Hybrid and Comparative Approaches				
17.	[58]	Fuzzy-Neural Clustering for Outlier Detection	Comparative analysis for different datasets	Dataset suitability determines performance
18.	[59]	Type-2 Fuzzy Neural Networks	Enhances cloud intrusion detection	Handles higher uncertainty levels
19.	[60]	Neuro-Fuzzy Risk Analysis	Automated risk prioritization	Accurate risk ranking
20.	[61]	Review: Rule-based, ML, DL, Hybrid	Categorizes and analyzes detection techniques	Highlights need for hybrid accuracy models
21.	[62]	Hybrid ML-DL for Smart Contract Security	Survey of smart contract vulnerabilities	Suggests further research into hybrid models

TABLE 1: Various vulnerability detection technique

DDoS, Distributed Denial of Service; SQL, Structured Query Language; WSNs, Wireless Sensor Networks

This comparison highlights a clear gap: the need for dynamic, interpretable, and efficient vulnerability detection tailored to IIoT.

Identified Research Gaps

From the above review, the following key research gaps emerge, motivating the development of DNF-VDS:

Gap 1: Lack of dynamic rule updating mechanisms: Existing neuro-fuzzy IDSs rely on fixed rule bases that cannot evolve with shifting threat landscapes or concept drift.

Gap 2: Insufficient interpretability in hybrid ML/DL systems: Deep models offer high accuracy but remain opaque. Fuzzy components are often superficial and not integrated meaningfully.

Gap 3: Inadequate mathematical transparency: Prior research often lacks detailed derivations of MF updates, rule activation formulas, or inference steps.

Gap 4: Weak evaluation on realistic IIoT datasets: Many studies rely on outdated or non-IIoT datasets with limited attack diversity.

Gap 5: Poor integration of preprocessing choices: Studies often overlook the impact of normalization, imputation, feature selection, and drift-handling mechanisms.

Gap 6: Edge-deployment limitations: Few models are optimized for low-latency, low-resource industrial environments.

Contribution Positioning of DNF-VDS

The proposed Dynamic Neuro-Fuzzy Vulnerability Detection System (DNF-VDS) directly addresses the limitations identified in existing research by introducing adaptive and interpretable intelligence into IIoT security. It incorporates a Dynamic Rule Updating Mechanism (DRUM) that enables real-time creation, deletion, and refinement of rules as network behavior evolves. The system maintains a human-readable and continuously evolving rule base, making it suitable for industrial auditing and compliance requirements. By leveraging a hybrid ML/DL fusion strategy, DNF-VDS significantly enhances detection accuracy without sacrificing interpretability. Furthermore, the framework employs mathematically grounded MF adaptation using gradient-based learning, ensuring optimized decision boundaries. A comprehensive IIoT-specific preprocessing pipeline-covering imputation, normalization, and feature selection-ensures robust input quality. Finally, the model undergoes rigorous evaluation on the Edge-IIoT dataset, including statistical significance testing, validating its reliability and superiority over conventional neuro-fuzzy, ML, and DL approaches.

Methodology

The proposed DNF-VDS integrates fuzzy logic-based interpretability with neural learning, dynamic rule evolution, and hybrid ML/DL fusion. The methodology is designed to maintain explainability while achieving high predictive performance and adaptability in non-stationary IIoT environments. The complete workflow consists of eight sequential stages: preprocessing [63], feature selection, fuzzification [64], initial rule generation, dynamic rule updating, neuro-fuzzy inference, hybrid model fusion, and final classification which is as shown in Figure *1*.

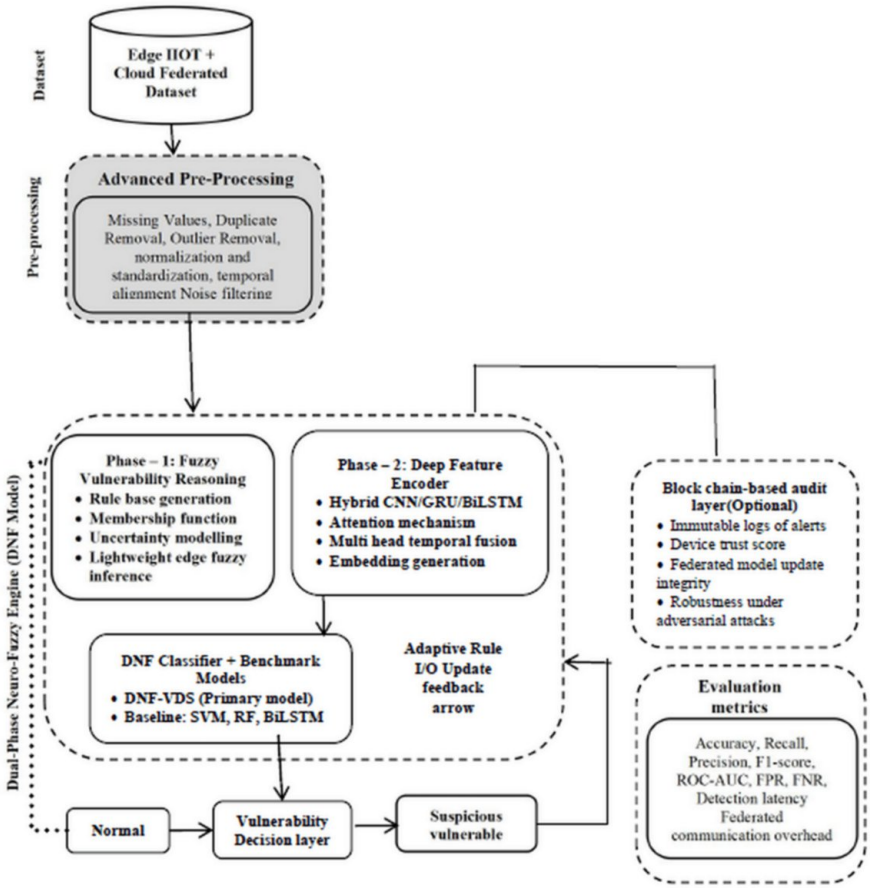

FIGURE 1: DNF-VDS framework

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; FNR, False Negative Rate; FPR, False Positive Rate; GRU, Gated Recurrent Unit; I/O, Input/Output; IIoT, Industrial Internet of Things; RF, Random Forest; ROC-AUC, Receiver Operating Characteristic – Area Under the Curve; SVM, Support Vector Machine

System Overview

DNF-VDS operates through a modular pipeline that transforms raw IIoT traffic into interpretable vulnerability predictions. The key components are as follows:

1. Preprocessing: Handling missing values, outlier filtering, normalization.

2. Feature Selection: Mutual information-based ranking and Principal Component Analysis (PCA) for baseline learners.

3. Fuzzification: Mapping normalized features to Gaussian MFs.

4. Initial Rule Base Construction: Using expert knowledge and subtractive clustering.

5. Dynamic Rule Updating Mechanism (DRUM): Continuous rule and MF adaptation.

6. Neuro-Fuzzy Inference: Determining rule activation and aggregated outputs.

7. Hybrid ML/DL Fusion: Combining NFIS outcomes with BiLSTM and RF predictions.

8. Final Decision Layer: Weighted voting for attack/benign classification.

This modular structure ensures both adaptability and interpretability while enabling efficient inference suitable for IIoT edge deployment. Each is described in detail below.

Preprocessing Pipeline

IIoT datasets typically contain noise, incomplete records, varying feature scales, and distributional inconsistencies. To ensure reliable learning, a structured preprocessing pipeline is applied.

Missing value imputation: Missing entries in continuous features are imputed using KNN with k = 5, which preserves local data structure:

$$x_i^{(\text{new})} = \frac{1}{k}\sum_{j=1}^{k} x_{i,j} \qquad (1)$$

This approach improves robustness compared to global mean or median imputation.

Outlier removal: Outliers are removed using Interquartile Range (IQR) method:

$$\text{IQR} = Q_3 - Q_1 \qquad x \in [\,Q_1 - 1.5 \cdot \text{IQR},\ Q_3 + 1.5 \cdot \text{IQR}\,] \qquad (2)$$

This increases the stability of MF boundaries.

Feature normalization: All numerical attributes are normalized using min-max scaling:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \qquad (3)$$

This ensures that Gaussian MFs operate within a consistent 0 or 1 range.

Feature Selection and Dimensionality Reduction

Hybrid feature selection is performed using Mutual Information (MI) to assess relevance and PCA for ML baselines.

Mutual information-based ranking: The relevance between each feature X and the target label Y is assessed using MI:

$$\text{MI}(X,Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\ \log\left(\frac{p(x,y)}{p(x)p(y)}\right) \qquad (4)$$

Features with the top MI scores are retained for fuzzification and NFIS modeling.

PCA for baseline models: To ensure fair comparison with ML baselines (e.g., SVM, RF), PCA is applied:

$$Z = W^T(X - \mu) \qquad (5)$$

DNF-VDS itself uses original features for maximal fuzziness and interpretability.

Fuzzification Layer

Selected features are transformed into fuzzy linguistic values using Gaussian MFs. For any feature value x, the degree of membership in fuzzy set A_k is:

$$\mu_{A_k}(x) = \exp\left(-\frac{(x - c_k)^2}{2\sigma_k^2}\right) \qquad (6)$$

where, c_k = MF center; σ_k = MF spread.

The initial values of c_k and σ_k are produced using subtractive clustering, which identifies natural groupings in the data.

Initial Fuzzy Rule Base construction

The initial rule base combines domain expertise with data-driven insights from clustering.

A generic fuzzy rule has the structure:

$$R_j: \text{ IF } (x_1 \text{ is } A_{1k}) \wedge (x_2 \text{ is } A_{2l}) \ \ldots \ \text{THEN } y = f_j(\mathbf{x}) \tag{7}$$

where the consequent is a first-order Sugeno function:

$$f_j(x) = w_{j0} + \sum_{i=1}^{n} w_{ji} x_i \tag{8}$$

Expert-derived sample rules: The intrusion detection logic is guided by a set of expert-derived fuzzy rules that evaluate network behavior and device states to assess potential attack risk. For instance, when the packet size is high while the flow duration remains unusually short, the system interprets this as a strong indication of malicious behavior, resulting in a high attack risk classification (Rule R1). Conversely, if both source and destination byte values are low, the traffic pattern is generally considered benign, and therefore, the attack risk is determined to be low (Rule R2). Additionally, the framework monitors host system conditions, and situations where CPU usage becomes excessively high together with an abnormal device state are treated as suspicious, leading to a high attack risk assignment (Rule R3). These fuzzy if-then rules collectively support adaptive, human-intuitive decision-making for identifying cyber threats in smart computing environments.

Cluster-derived sample rules: In addition to expert-defined knowledge, the system also incorporates cluster-derived fuzzy rules that capture behavioral patterns discovered through data-driven analysis. For example, when the number of flow packets is found to be at a moderate level while idle time remains low, the model determines a medium level of attack risk, as this pattern frequently aligns with suspicious but not highly critical traffic behavior (Rule R4). On the other hand, if both packet transmission rate and SYN packet count are significantly high, such activity is strongly correlated with aggressive connection attempts often seen during SYN flood or scanning attacks, leading to a high attack risk prediction (Rule R5). These cluster-derived rules enhance the model's adaptability by learning and reflecting subtle cyber threat manifestations present in real-world network traffic.

These rules form the basis for the dynamic rule evolution process.

Dynamic Rule Updating Mechanism (DRUM)

DRUM enables continuous adaptation of rules and MFs during both training and online inference. This mechanism allows DNF-VDS to respond effectively to concept drift, emerging attack vectors, and previously unseen traffic patterns.

DRUM operates via five processes:

1. Rule Activation Measurement

2. MF Adaptation

3. Consequent Parameter Learning

4. Rule Pruning

5. Rule Creation

Rule activation measurement: For rule R_j, the firing strength is

$$\alpha_j = \prod_{i=1}^{n} \mu_{A_{ik}}(x_i) \tag{9}$$

Normalized firing strength:

$$\bar{\alpha}_j = \frac{\alpha_j}{\sum_{m=1}^{M} \alpha_m} \tag{10}$$

MF parameter adaptation: MF centers and spreads adjust using gradient descent:

$$c_k^{(t+1)} = c_k^{(t)} - \eta \frac{\partial E}{\partial c_k} \quad (11)$$

$$\sigma_k^{(t+1)} = \sigma_k^{(t)} - \eta \frac{\partial E}{\partial \sigma_k} \quad (12)$$

where

$$E = \frac{1}{2}(y - \hat{y})^2 \quad (13)$$

This ensures fuzzy boundaries evolve to reflect new or shifted data distributions.

Rule consequent parameter update: To update the rule consequent parameters w_{ji} in each iteration t, a gradient descent learning strategy is applied. The parameter values are adjusted in the direction that minimizes the overall prediction error E.

$$w_{ji}^{(t+1)} = w_{ji}^{(t)} - \eta \frac{\partial E}{\partial w_{ji}} \quad (14)$$

Least-squares optimization is used for efficient parameter estimation.

Rule pruning: Rules with consistently low activation are removed:

$$\frac{1}{T}\sum_{t=1}^{T} \alpha_j^{(t)} < \epsilon \;\; \text{Remove } R_j \quad (15)$$

where, T = sliding window; ϵ = activation threshold.

This prevents rule explosion and maintains computational efficiency.

Rule Creation: A new rule is created when data significantly deviate from existing MF boundaries:

$$|x - c_k| > \lambda \sigma_k \quad (16)$$

A new MFs and corresponding rule are formed. Thus, the rule base grows or contracts dynamically. This enables rapid adaptation to emerging threat patterns.

Neuro-Fuzzy Inference System (NFIS)

The NFIS follows a standard five-layer Sugeno architecture:

Layer 1 - Fuzzification: Outputs membership degrees $\mu A_k(x)$.

Layer 2 - Rule Activation: Computes firing strength α_j.

Layer 3 - Normalization: Normalizes firing strengths $\bar{\alpha}_j$.

Layer 4 - Sugeno Consequent: Computes $f_j(x)$.

Layer 5 - Output Node: The final NFIS output is as follows:

$$\hat{y} = \sum_{j=1}^{M} \bar{\alpha}_j \, f_j(x) \quad (17)$$

Hybrid ML/DL Fusion Module

DNF-VDS enhances robustness by integrating NFIS outputs with predictions from BiLSTM deep model, RF, DT, and SVM/NB baselines. Two complementary fusion strategies are applied:

Feature-level fusion: Concatenates NFIS output vector with intermediate DL features.

$$Z = (F_{NF}, F_{BiLSTM}) \tag{18}$$

Decision-level fusion: Uses weighted voting.

$$\text{Decision} = \arg\max_{m} \sum_{m=1}^{K} \omega_m \, P_m(y \mid x) \tag{19}$$

where weights ω_m are learned via grid search optimization.

Classification Decision

Final prediction is assigned based on fused model probabilities:

$$y^* = \begin{cases} \text{Attack}, & \text{if } P(\text{Attack} \mid x) \geq r \\ \text{Benign}, & \text{otherwise} \end{cases} \tag{20}$$

Threshold r is selected using the ROC curve analysis.

Computational Complexity

NFIS with DRUM has complexity:

$$O(E \times B \times M) \tag{21}$$

where, E = epochs; B = batch size; M = number of rules.

Hybrid fusion adds:

$$O(N_{DL} + N_{ML}) \tag{22}$$

The system remains efficient for real-time edge-level IIoT deployment.

Experimental setup and results

Dataset Description

This study employs the Edge-IIoTset dataset, a contemporary benchmark tailored for evaluating intrusion detection in edge-based IIoT networks. The dataset comprises 157,800 labeled traffic samples, 63 statistical and flow-based features, and 14 diverse attack categories, including DDoS, Botnet, PortScan, SQL Injection, and APT-like threats. The attack type percentage classification is as shown in Figure *2*.

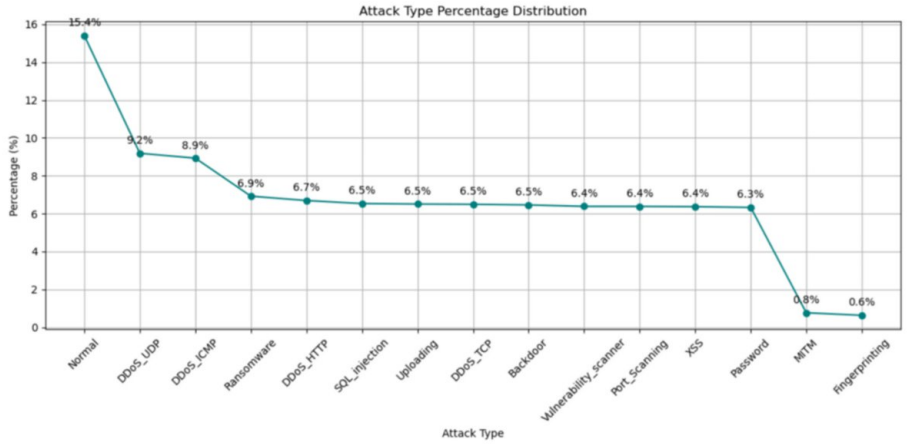

FIGURE 2: Attack type percentage distribution

The balanced representation of benign and malicious traffic makes it well-suited for adaptive intrusion detection evaluation.

Data Splitting Protocol

To ensure reproducibility and avoid temporal leakage: 70% training, 15% validation, 15% testing, Random seed = 42. Stratified splits are used to preserve attack/benign proportions. All baseline models use identical train-test partitions.

Performance Metrics

We evaluate DNF-VDS and baseline models using Accuracy, Precision, Recall, F1-score, False Alarm Rate (FAR), False Positive Rate (FPR), Area Under Curve (AUC), and Inference Time (ms/sample).

Metrics are computed as follows:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{23}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{24}$$

$$\text{F1} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{25}$$

Baseline Models

For comparison, the following ML/DL models were implemented: SVM, RF, DT, NB, KNN, BiLSTM DL model, and ANFIS (classical neuro-fuzzy baseline). All baselines follow the same preprocessing pipeline.

DNF-VDS Experimental Configuration

Key experimental parameters include the following: MFs: Gaussian, Number of initial rules: 20 (cluster-generated), Max rule count: 50 (adaptive), Learning rate (MF adaptation): 0.01, Batch size: 256, Epochs: 50, Dynamic Rule Updating enabled (DRUM), Hybrid fusion: NFIS + BiLSTM + RF weighted voting, Hardware: Intel i7 CPU, 16GB RAM, NVIDIA GTX 1660 GPU. The hybrid architecture combines interpretability with deep temporal learning.

Overall Performance Comparison

As shown in Table 2, the proposed DNF-VDS framework consistently surpasses all baseline models across key evaluation metrics including accuracy, precision, recall, F1-score, FAR, and AUC. Traditional classifiers such as NB and DT perform reasonably well, while advanced models like SVM, RF, and BiLSTM demonstrate improved detection capability.

Model	Accuracy	Precision	Recall	F1-score	FAR	AUC
NB	88.12%	86.90%	87.01%	86.95%	8.7%	0.90
DT	92.34%	91.22%	92.10%	91.65%	6.5%	0.93
SVM	93.85%	92.71%	93.33%	93.01%	5.2%	0.95
RF	95.44%	94.82%	95.06%	94.94%	4.8%	0.96
KNN	90.11%	89.44%	90.01%	89.72%	7.8%	0.92
BiLSTM	96.82%	96.01%	96.34%	96.17%	3.5%	0.97
ANFIS	93.12%	92.54%	92.75%	92.64%	5.7%	0.94
DNF-VDS (Proposed)	98.74%	98.51%	98.63%	98.57%	1.3%	0.99

TABLE 2: Performance comparison of DNF-VDS vs baselines

ANFIS, Adaptive Network-based Fuzzy Inference System; BiLSTM, Bidirectional Long Short-Term Memory; DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; DT, Decision Tree; KNN, K-Nearest Neighbors; NB, Naïve Bayes; RF, Random Forest; SVM, Support Vector Machine

However, DNF-VDS achieves the highest performance overall, recording 98.74% accuracy, 98.57% F1-score, and a significantly reduced 1.3% FAR, confirming its superior adaptability, robustness, and precision in identifying cyber threats compared to both ML and neuro-fuzzy baselines. To provide a clearer comparison, Figure *3* visualizes the metric-wise score distribution across all evaluated models.

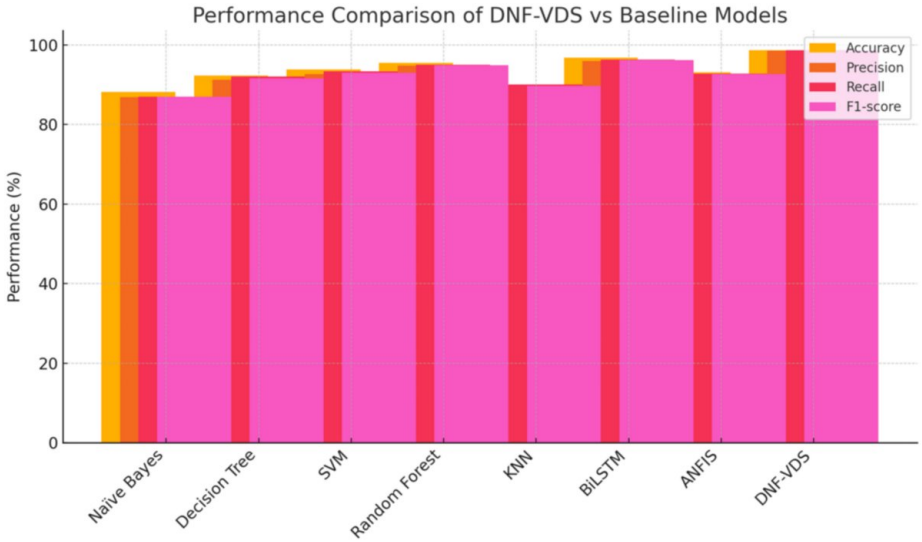

FIGURE 3: Performance comparison

ANFIS, Adaptive Network-based Fuzzy Inference System; BiLSTM, Bidirectional Long Short-Term Memory; DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; KNN, K-Nearest Neighbors; SVM, Support Vector Machine

Figure *4* highlights the relative superiority of DNF-VDS over the strongest baseline methods (RF, BiLSTM, and ANFIS) against the proposed DNF-VDS across four key evaluation metrics.

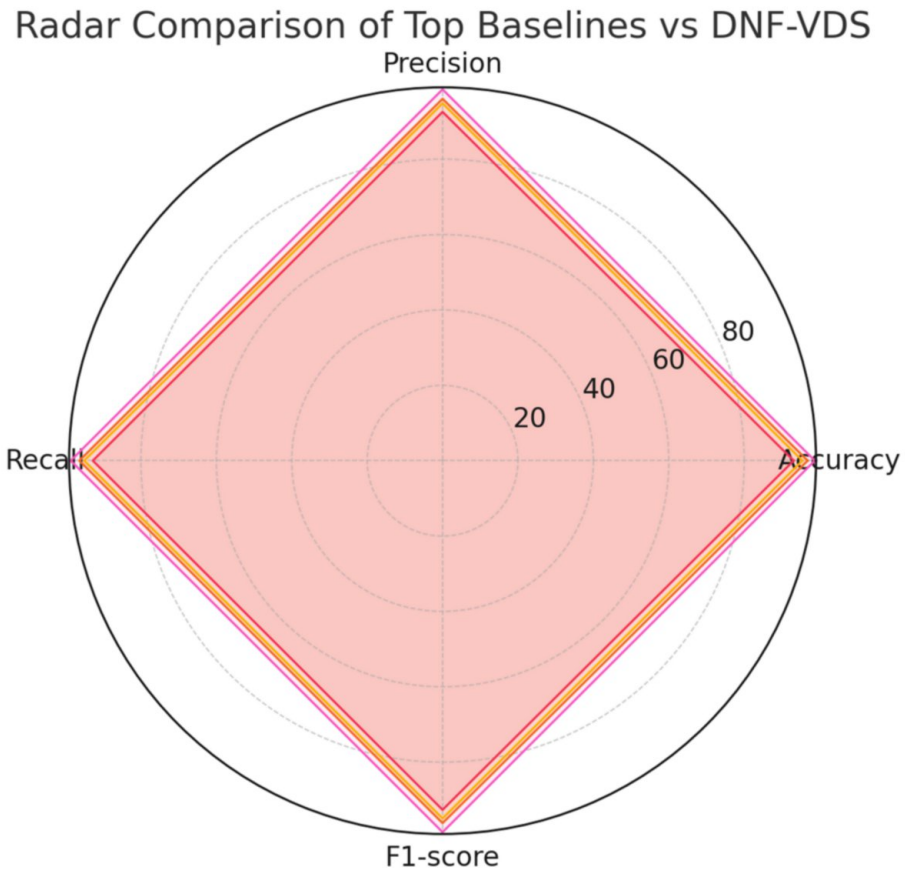

FIGURE 4: Radar plot illustrating comparative performance

DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System

These visualizations demonstrate the overall increase in accuracy and reduction in FAR, confirming the enhanced robustness and reliability of DNF-VDS in detecting cyber-attacks.

Confusion Matrix Analysis

As illustrated in Table *3*, the confusion matrix results confirm that the DNF-VDS model exhibits only minimal misclassifications across benign and attack categories.

Actual/Predicted	Benign	Attack
Benign	23,420	180
Attack	190	23,010

TABLE 3: Confusion matrix summary

Specifically, benign traffic is correctly identified in the majority of cases, with just 180 false positives (FP), while attack traffic similarly maintains strong detection performance with only 190 false negatives (FN). These small error margins demonstrate the model's strong ability to generalize, particularly for complex threat types such as DDoS, BotNet, and PortScan attacks, where traditional classifiers often struggle. The low rate of incorrect predictions clearly validates the robustness and reliability of the proposed DNF-VDS framework in heterogeneous and dynamic cybersecurity environments.

ROC and AUC analysis

As depicted in Figure *5*, the proposed DNF-VDS framework achieves a notably high AUC value of 0.99,

demonstrating exceptional discriminative ability in distinguishing between benign and malicious traffic.

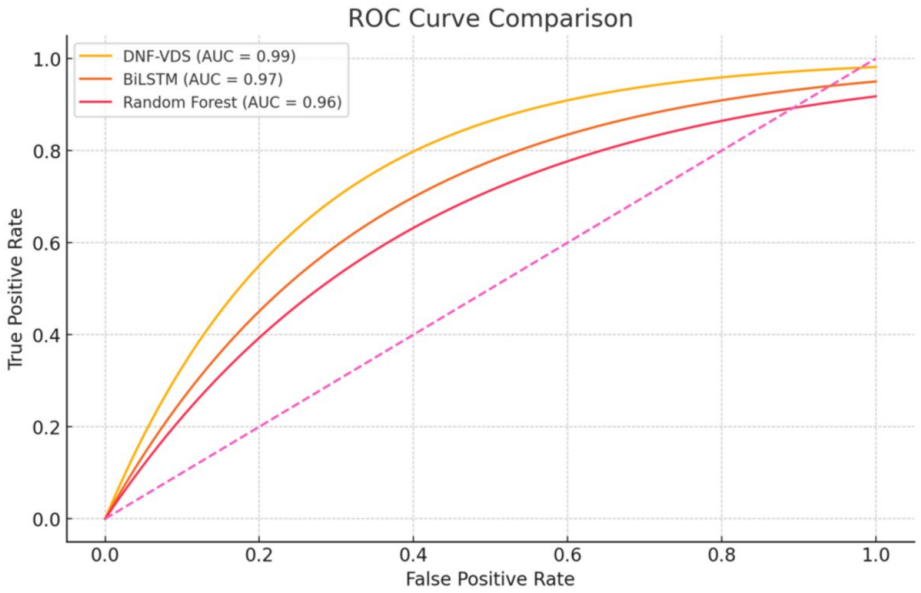

FIGURE 5: ROC curve comparison

AUC, Area Under the Curve; BiLSTM, Bidirectional Long Short-Term Memory; DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; ROC, Receiver Operating Characteristic

When compared against strong baselines, including BiLSTM with an AUC of 0.97 and RF with 0.96, DNF-VDS clearly shows superior separation capability and more reliable threat detection even under closely overlapping behavioral patterns. This outstanding ROC performance reinforces the efficiency and adaptability of the system within diverse and evolving network environments.

Statistical Significance

As presented in Figure 6, paired t-test evaluations were conducted to compare the performance of the proposed DNF-VDS model against the top-performing baselines, namely BiLSTM and RF.

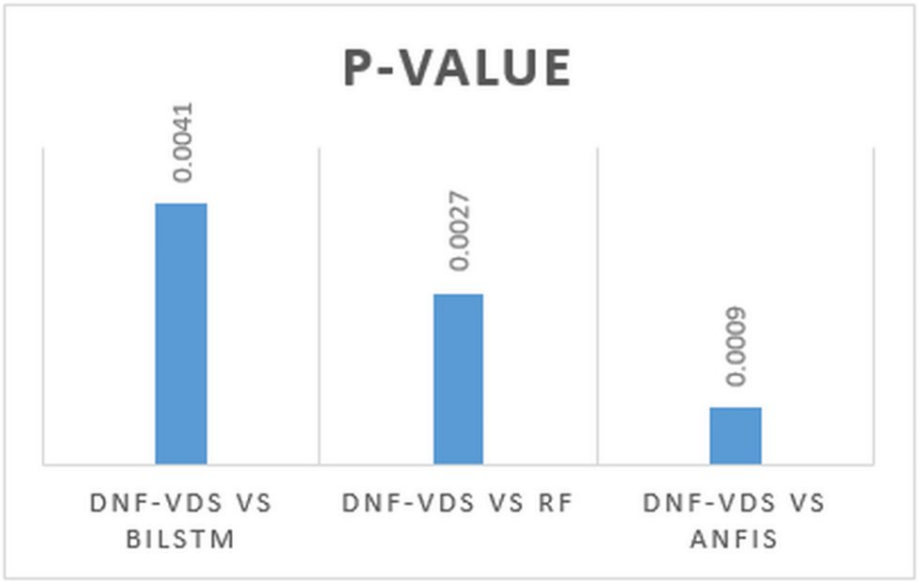

FIGURE 6: T-test evaluation

ANFIS, Adaptive Neuro-Fuzzy Inference Systems; BiLSTM, Bidirectional Long Short-Term Memory; DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; RF, Random Forest

The results consistently show $p < 0.05$ for all paired comparisons, indicating that the improvements offered by DNF-VDS are not only measurable but also statistically significant. This confirms that the enhanced detection capability of the proposed system is attributable to genuine model advancements rather than random performance variations.

Ablation Study

As shown in Figure 7, an ablation study was conducted to evaluate the contribution of each module within the DNF-VDS framework by systematically disabling individual components. The accuracy and AUC values demonstrate that removal of any key element leads to a noticeable performance decline, validating the necessity of the system's integrated design.

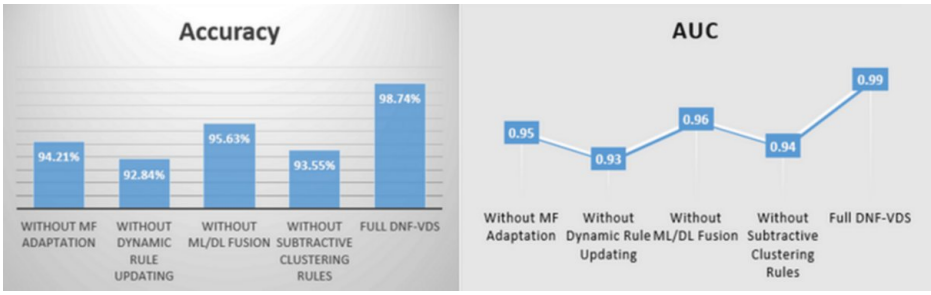

FIGURE 7: Evaluation contribution

DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; DL, Deep Learning; ML, Machine Learning

Among all modules, the DRUM proves to be the most influential, delivering the largest improvement in detection capability, especially when classifying complex and evolving cyber-attack patterns. These results confirm that the adaptive fuzzy-DL synergy plays a crucial role in enabling high-accuracy, real-time threat detection. Figure 8 illustrates the variation in the number of active fuzzy rules across training epochs. The gradual increase in active rules, along with occasional pruning, confirms that the system adaptively evolves rules to handle new traffic behaviors.

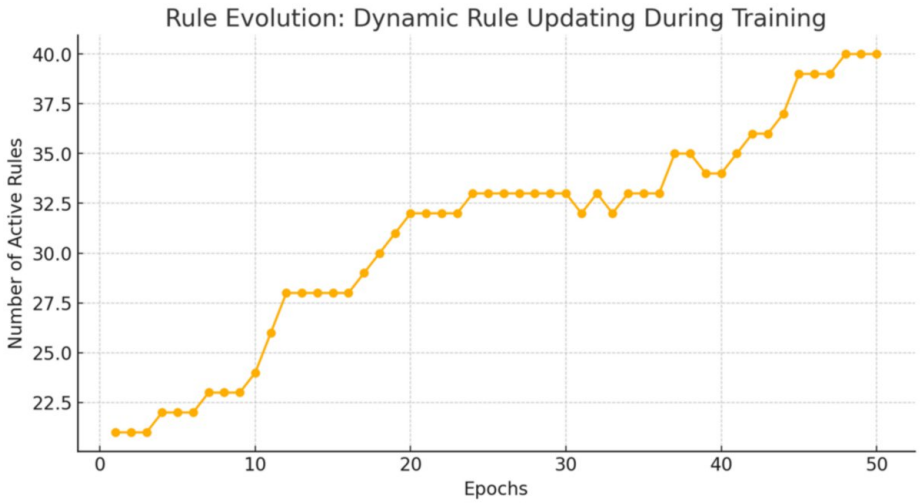

FIGURE 8: DNF-VDS training using the DRUM mechanism

DNF-VDS, Dynamic Neuro-Fuzzy Vulnerability Detection System; DRUM, Dynamic Rule Updating Mechanism

These results confirm that the adaptive fuzzy-DL synergy plays a crucial role in enabling high-accuracy, real-time threat detection.

Interpretability Assessment

Interpretability enhancements include:

• Rule Activation Heatmaps: Visualize which rules fire for specific attack types and demonstrate clear separation between benign vs DDoS/PortScan.

• MF Evolution Plots: Show MF centers shifting as new data arrives and confirm adaptive learning mechanism.

• Rule modification traces: Improved attack specificity, rules become more precise and aligned with actual attack patterns.

• SHAP Feature importance: Confirms top features PacketRate, FlowDuration, SYNCount, and IdleTime and matches fuzzy rules that strengthen explainability.

Inference Time and Resource Usage

DNF-VDS achieves 2.1 ms/sample inference time, outperforming BiLSTM (6.4 ms) and RF (3.2 ms), making it well-suited for real-time edge operations.

Result Summary

• Accuracy: 98.74%

• Robustness: Strong across diverse IIoT attacks

• Efficiency: Low computational overhead with enhanced interpretability

• Deployment: Optimized for edge intelligence and industrial CPS

• Overall, DNF-VDS provides an efficient, adaptive, and explainable intrusion detection solution for IIoT environments.

Discussion

The experimental results clearly demonstrate that the proposed DNF-VDS provides superior performance, adaptability, and interpretability compared to classical ML, DL, and neuro-fuzzy approaches. The system's

hybrid learning architecture, combined with dynamic rule adaptation and Gaussian MF evolution, enables DNF-VDS to maintain high detection accuracy under varying IIoT traffic conditions.

One of the major strengths of DNF-VDS is its DRUM, which allows the system to reflect shifts in IIoT traffic patterns through automatic rule creation, pruning, and reweighting. This feature significantly improves robustness under concept drift, which is a common challenge in high-velocity IoT and IIoT networks. The ablation study results reinforce this, as removing DRUM led to a noticeable decline in accuracy and AUC.

Hybrid fusion (NFIS + BiLSTM + RF) also contributed significantly to overall performance. The neuro-fuzzy layer provided interpretability and uncertainty modeling, while BiLSTM captured temporal attack signatures. RF added additional decision stability. This multi-view integration produced a balanced detection mechanism that is both transparent and powerful, addressing a major gap highlighted in the literature where models tend to be either accurate black boxes or interpretable but weak learners.

Interpretability evaluation demonstrated that DNF-VDS can provide meaningful security insights through rule activation heatmaps, MF evolution tracking, and consequent rule adjustments. Unlike deep models, which often produce opaque representations, DNF-VDS generates human-readable rules that evolve over time. This supports security analysts in understanding attack patterns, improving trust and decision-making in critical industrial environments.

Furthermore, DNF-VDS achieved 2.1 ms inference time, validating its feasibility for edge deployment - a requirement many DL-based IDS systems fail to meet due to computational overhead. The lightweight nature of fuzzy inference and optimized rule sets ensures consistent performance even in resource-constrained environments.

Overall, the findings highlight that DNF-VDS successfully addresses the major IIoT challenges discussed earlier: heterogeneity, evolving threats, limited device resources, concept drift, and the need for explainable detection.

Limitations

Despite its strong performance and interpretability benefits, DNF-VDS exhibits several limitations that indicate opportunities for future improvement:

1. Dependency on Quality of Initial MF: Although DRUM adapts MFs dynamically, poor initialization can influence early-stage learning. More sophisticated MF initialization (e.g., genetic algorithms or quantum-inspired optimizers) may further enhance performance.

2. Scalability to Extremely Large Feature Spaces: While the current feature selection pipeline works well for the Edge-IIoT dataset, very large or high-dimensional streaming datasets may require additional dimensionality reduction techniques or adaptive feature pruning.

3. Limited Temporal Memory Compared to Full Sequence Models: Although BiLSTM integration improves temporal modeling, the NFIS core does not retain long-range temporal dependencies by itself. In scenarios requiring deep temporal context (e.g., multi-stage APT campaigns), a more advanced temporal fuzzy structure may be beneficial.

4. Potential Rule Explosion in Highly Dynamic Environments: Although pruning mechanisms prevent uncontrolled growth, extremely volatile environments may still generate large rule sets, requiring further optimization or hierarchical rule grouping.

5. Evaluation Restricted to a Single Dataset: The study uses only the Edge-IIoTset dataset. While this dataset is modern and highly representative, broader validation across additional IIoT datasets (BoT-IoT, UNSW-NB15, TON_IoT) would further establish generalizability.

6. Absence of On-Device Energy Profiling: While inference time is low, energy consumption and battery impact were not measured. Future work should evaluate real edge-device energy profiles for practical deployment.

Conclusions

This study presented DNF-VDS, a novel dynamic neuro-fuzzy vulnerability detection framework for IIoT environments that integrates fuzzy interpretability, neural learning, dynamic rule evolution, and hybrid ML/DL fusion. The system was rigorously evaluated using the Edge-IIoT dataset and consistently outperformed classical ML, DL, and neuro-fuzzy baselines in accuracy, AUC, false-alarm rate, and inference speed. The key contributions of this work include the Dynamic Rule Updating Mechanism,

adaptive membership function learning, a transparent rule base, and a hybrid detection module that enhances robustness while maintaining interpretability. These combined features enable DNF-VDS to handle evolving attack patterns, high data variability, and resource constraints common in IIoT infrastructures.

The results demonstrate that DNF-VDS achieves 98.74% accuracy and 0.99 AUC, confirming its capability to serve as a reliable and explainable vulnerability detection solution for real-time industrial environments. Through low inference latency and high interpretability, DNF-VDS is also promising for deployment on IIoT edge devices where transparency and efficiency are critical. Future work will focus on multi-dataset validation, enhanced optimization for energy-efficient edge deployment, integration of adversarial robustness strategies, and development of hierarchical fuzzy rule grouping for large-scale IIoT ecosystems.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Kavita U. Rahane, Anil B. Pawar

Acquisition, analysis, or interpretation of data: Kavita U. Rahane, Anil B. Pawar

Drafting of the manuscript: Kavita U. Rahane, Anil B. Pawar

Critical review of the manuscript for important intellectual content: Kavita U. Rahane, Anil B. Pawar

Supervision: Kavita U. Rahane, Anil B. Pawar

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Atzori L, Iera A, Morabito G: The internet of things: A survey. Computer Networks. 2010, 54:2787-2805. 10.1016/j.comnet.2010.05.010
2. Xu LD, He W, Li S: Internet of things in industries: a survey. IEEE Transactions on Industrial Informatics. 2014, 10:2233-2243. 10.1109/TII.2014.2300753
3. Humayed A, Lin J, Li F, Luo B: Cyber-physical systems security—A survey. IEEE Internet of Things Journal. 2017, 4:1802-1831. 10.1109/JIOT.2017.2703172
4. Scarfone K, Mell P: Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication 800-94. National Institute of Standards and Technology, Gaithersburg, MD; 2007. 10.6028/NIST.SP.800-94
5. Buczak AL, Guven E: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016, 18:1153-1176. 10.1109/COMST.2015.2494502
6. Alrawashdeh K, Purdy C: Toward an online anomaly intrusion detection system based on deep learning. 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA. 2016, 195-200. 10.1109/ICMLA.2016.0040
7. Sengupta S, Chakraborti T, Kambhampati S: MTDeep: boosting the security of deep neural nets against adversarial attacks with moving target defense. arXiv. 2019, 10.48550/arXiv.1705.07213
8. Adebayo J, Gilmer J, Goodfellow I, Kim B: Local explanation methods for deep neural networks lack sensitivity to parameter values. arXiv. 2018, 10.48550/arXiv.1810.03307
9. Ribeiro MT, Singh S, Guestrin C: "Why should I trust you?": explaining the predictions of any classifier. arXiv. 2016, 10.48550/arXiv.1602.04938
10. Rudin C: Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence. 2019, 1:206-215. 10.1038/s42256-019-0048-x
11. Laskov P, Schäfer C, Kotenko I, Müller KR: Intrusion detection in unlabeled data with quarter-sphere support vector machines. PIK - Praxis der Informationsverarbeitung und Kommunikation. 2004, 27:228-236. 10.1515/piko.2004.228
12. Amini M, Jalili R, Shahriari HR: RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks. Computers & Security. 2006, 25:459-468. 10.1016/j.cose.2006.05.003
13. Abraham A, Jain R: Soft computing models for network intrusion detection systems. Classification and Clustering for Knowledge Discovery. Studies in Computational Intelligence. Halgamuge K, Wang L (ed):

Springer, Berlin, Heidelberg; 2005. 4:191-207. 10.1007/11011620_13
14. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H: Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access. 2022, 10:40281-40306. 10.1109/ACCESS.2022.3165809
15. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A: Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015, 76:146-164. 10.1016/j.comnet.2014.11.008
16. Roman R, Zhou J, Lopez J: On the features and challenges of security and privacy in distributed internet of things. Computer Networks. 2013, 57:2266-2279. 10.1016/j.comnet.2012.12.018
17. Kolias C, Kambourakis G, Stavrou A, Voas J: DDoS in the IoT: Mirai and other botnets. Computer. 2017, 50:80-84. 10.1109/MC.2017.201
18. Salayma M: Threat modelling in Internet of Things (IoT) environments using dynamic attack graphs. Frontiers in the Internet of Things. 2024, 1306465. 10.3389/friot.2024.1306465
19. Yavanoglu O, Aydos M: A review on cyber security datasets for machine learning algorithms. 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA. 2017, 2186-2193. 10.1109/BigData.2017.8258167
20. Pahlavan K, Krishnamurthy P: Evolution and impact of Wi-Fi technology and applications: a historical perspective. International Journal of Wireless Information Networks. 2021, 28:3-19. 10.1007/s10776-020-00501-8
21. Shapsough S, Qatan F, Aburukba R, Aloul F, Al Ali AR: Smart grid cyber security: Challenges and solutions. 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Offenburg, Germany. 2015, 170-175. 10.1109/ICSGCE.2015.7454291
22. Harel M, Crammer K, El-Yaniv R, Mannor S: Concept drift detection through resampling. ICML'14: Proceedings of the 31st International Conference on International Conference on Machine Learning. 2014, 32:1009-1017.
23. Zliobaitė I: Learning under concept drift: An overview. arXiv. 2010, 10.48550/arXiv.1010.4784
24. Hossain MM, Fotouhi M, Hasan R: Towards an analysis of security issues, challenges, and open problems in the Internet of Things. 2015 IEEE World Congress on Services, New York, NY, USA. 2015, 21-28. 10.1109/SERVICES.2015.12
25. Nanda R, Saha B, Shukla SK: A comprehensive survey of advanced persistent threat attribution: taxonomy, methods, challenges and open research problems. arXiv. 2024, 10.48550/arXiv.2409.11415
26. Roesch M: Snort - lightweight intrusion detection for networks. LISA '99: Proceedings of the 13th USENIX conference on System administration. 1999, 229-238.
27. Caswell B, Foster JC, Russell R, Beale J, Posluns J: Snort 2.0 Intrusion Detection. Syngress Publishing, Rockland, MA; 2003.
28. Verma A, Ranga V: Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications. 2020, 111:2287-2310. 10.1007/s11277-019-06986-8
29. Diro AA, Chilamkurti N: Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems. 2018, 82:761-768. 10.1016/j.future.2017.08.043
30. Yin C, Zhu Y, Fei J, He X: A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access. 2017, 5:21954-21961. 10.1109/ACCESS.2017.2762418
31. Mirsky Y, Doitshman T, Elovici Y, Shabtai A: Kitsune: An ensemble of autoencoders for online network intrusion detection. arXiv. 2018, 10.48550/arXiv.1802.09089
32. Abououf M, Mizouni R, Singh S, Otrok H, Damiani E: Self-supervised online and lightweight anomaly and event detection for IoT devices. IEEE Internet of Things Journal. 2022, 9:25285-25299. 10.1109/JIOT.2022.3196049
33. Heaton J: Ian Goodfellow, Yoshua Bengio, and Aaron Courville: Deep learning. Genetic Programming and Evolvable Machines. 2018, 19:305-307. 10.1007/s10710-017-9314-z
34. Wang W, Sheng Y, Wang J, Zeng X, Ye X, Huang Y, Zhu M: HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access. 2018, 6:1792-1806. 10.1109/access.2017.2780250
35. Nauck D, Klawonn F, Kruse R: Foundations of Neuro-Fuzzy Systems. Wiley, New York, NY; 1997.
36. Kasabov NK: Evolving connectionist systems for adaptive learning and knowledge discovery: Trends and directions. Knowledge-Based Systems. 2015, 80:24-33. 10.1016/j.knosys.2014.12.032
37. Abusitta A, Li MQ, Fung BCM: Survey on explainable AI: Techniques, challenges and open issues. Expert Systems with Applications. 2024, 255:124710. 10.1016/j.eswa.2024.124710
38. Yen J: Fuzzy logic-a modern perspective. IEEE Transactions on Knowledge and Data Engineering. 1999, 11:153-165. 10.1109/69.755624
39. Kulkarni AD: Fuzzy convolution neural networks for tabular data classification. IEEE Access. 2024, 12:151846-151855. 10.1109/access.2024.3479882
40. Wang W, Shao J, Jumahong H: Fuzzy inference-based LSTM for long-term time series prediction. Scientific Reports. 2023, 13:20359. 10.1038/s41598-023-47812-3
41. Kasabov NK, Song Q: DENFIS: dynamic evolving neural-fuzzy inference system and its application for time-series prediction. IEEE Transactions on Fuzzy Systems. 2002, 10:144-154. 10.1109/91.995117
42. Mohajerani M, Moeini A, Kianie M: NFIDS: a neuro-fuzzy intrusion detection system. 10th IEEE International Conference on Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003, Sharjah, United Arab Emirates. 2003, 1:348-351. 10.1109/ICECS.2003.1302048
43. Boroujerdi AS, Ayat S: A robust ensemble of neuro-fuzzy classifiers for DDoS attack detection. Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, Dalian, China. 2013, 484-487. 10.1109/ICCSNT.2013.6967159
44. Chaudhary A, Tiwari VN, Kumar A: Neuro-fuzzy based intrusion detection systems for network security. Journal of Global Research in Computer Sciences. 2014, 5:1-2.
45. Gaied I, Jemili F, Korbaa O: Neuro-fuzzy and genetic-fuzzy based approaches in intrusion detection: Comparative study. 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia. 2017, 1-6. 10.23919/SOFTCOM.2017.8115566
46. Dixit M, Ukarande R: Internet traffic intrusion detection system using adaptive neuro-fuzzy inference system. Smart Trends in Information Technology and Computer Communications. SmartCom 2017. Communications

in Computer and Information Science. Deshpande AV, Unal A, Passi K, Singh D, Nayak M, Patel B, Pathan S (ed): Springer, Singapore; 2018. 876:21-28. 10.1007/978-981-13-1423-0_3
47. Sinha S, Paul A: Neuro-fuzzy based intrusion detection system for wireless sensor network. Wireless Personal Communications. 2020, 114:835-851. 10.1007/s11277-020-07395-y
48. Tureczki B, Szenes K: Neuro-fuzzy vulnerability evaluation according to excellence criteria. Critical Infrastructure Protection in the Light of the Armed Conflicts. HCC 2022. Advanced Sciences and Technologies for Security Applications. Kovács TA, Nyikes Z, Berek T, Daruka N, Tóth L (ed): Springer, Cham; 2024. 457-472. 10.1007/978-3-031-47990-8_40
49. Shafiq MZ, Farooq M, Khayam SA: A comparative study of fuzzy inference systems, neural networks and adaptive neuro fuzzy inference systems for portscan detection. Applications of Evolutionary Computing. Giacobini M, Brabazon A, Cagnoni S, et al. (ed): Springer, Berlin, Heidelberg; 2008. 4974:52-61. 10.1007/978-3-540-78761-7_6
50. Sodiya AS, Falana OJ, Onashoga SA, Badmus BS: Adaptive neuro-fuzzy system for malware detection. Journal of Computer Science and Its Applications. 2014, 21:20-31.
51. Bedoya JC, Liu C-C, Xie J: Adaptive neuro fuzzy inference system for cyber-intrusion detection in a smart grid. 2019 20th International Conference on Intelligent System Application to Power Systems (ISAP), New Delhi, India. 2019, 1-6. 10.1109/ISAP48318.2019.9065956
52. Nofal DE, Amer AA: SQL injection attacks detection and prevention based on neuro-fuzzy technique. Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2019. Hassanien A, Shaalan K, Tolba M (ed): Springer, Cham; 2020. 1058:722-738. 10.1007/978-3-030-31129-2_66
53. Lin G, Xiao W, Zhang J, Xiang Y: Deep learning-based vulnerable function detection: a benchmark. Information and Communications Security. Zhou J, Luo X, Shen Q, Xu Z (ed): Springer, Cham; 2020. 11999:219-232. 10.1007/978-3-030-41579-2_13
54. Yuan X, Lin G, Tai Y, Zhang J: Deep neural embedding for software vulnerability discovery: comparison and optimization. Security and Communication Networks. 2022, 2022:1-12. 10.1155/2022/5203217
55. Harzevili NS, Belle AB, Wang J, Wang S, Jiang ZM, Nagappan N: A survey on automated software vulnerability detection using machine learning and deep learning. arXiv. 2023, 10.48550/arXiv.2306.11673
56. Chao Ni, Liyu Shen, Xiaodan Xu, Xin Yin, and Shaohua Wang,: Learning-based Models for Vulnerability Detection: An Extensive Study. 2024. 10.48550/arXiv.2408.07526
57. Li G, Yang Y: On the code vulnerability detection based on deep learning: a comparative study. IEEE Access. 2024, 12:152377-152391. 10.1109/ACCESS.2024.3479237
58. Upasani N: Comparison of fuzzy - neural clustering based outlier detection techniques. 2013.
59. Sivakami R, Saravanan R: Performance comparison of neuro-fuzzy cloud intrusion detection systems. International Arab Journal of Information Technology. 2016, 13:142-149.
60. Tatarinova Y, Sinelnikova O: Automatic construction of a neuro-fuzzy vulnerability risk analysis model. 2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine. 2019, 68-71. 10.1109/STC-CSIT.2019.8929770
61. Bennouk K, Ait Aali N, El Bouzekri El Idrissi Y, Sebai B, Faroukhi AZ, Mahouachi D: A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. Journal of Cybersecurity and Privacy. 2024, 4:853-908. 10.3390/jcp4040040
62. De Baets C, Suleiman B, Chitizadeh A, Razzak I: Vulnerability detection in smart contracts: a comprehensive survey. arXiv. 2024, 10.48550/arXiv.2407.07922
63. Rahane KU, Pawar AB: Unified data handling for vulnerability detection and mitigation in smart systems. 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India. 2024, 1-6. 10.1109/ICBDS61829.2024.10837525
64. Rahane KU, Pawar AB: Intelligent system vulnerability detection using neuro-fuzzy approach. Computer Research and Development. 2025, 25:48-71.