Computer Networks and Communications
http://ojs.wiserpub.com/index.php/CNC/

Research Article

A Novel Soft Computing-Driven Entropy-Fuzzy Rule Optimization Framework for Early Adaptive Intrusion Detection

Sandeep Bhattacharjee

Amity Business School, Amity University Kolkata, Newtown 700135, India
Correspondence: sandeepbitmba@gmail.com

Received: 14 January 2026; **Revised:** 10 March 2026; **Accepted:** 25 March 2026; **Published:** 1 April 2026

Abstract: This paper proposes the Entropy-Fuzzy Rule Optimized Synergistic Tuning Framework for Intrusion Detection System (E-FROST IDS), an entropy-driven, fuzzy-rule-optimization-enhanced intrusion detection system designed to address challenges related to model accuracy, flexibility, and uncertainty. The results suggest that E-FROST improves the effectiveness of anomaly detection, reduces false alarms, and enhances interpretability through entropy-based uncertainty modeling. The novelty lies in integrating fuzzy entropy with an efficient decision engine tailored for dynamic threat environments. The main contribution is a unified and adaptive IDS capable of identifying threats across a wide range of network conditions. Major implications include strengthened cyber-defense preparedness, greater transparency for security analysts, and a flexible framework for future intelligent intrusion detection system solutions.

***Keywords*:** cybersecurity, entropy modeling, fuzzy logic, Intrusion Detection System (IDS), optimization framework, uncertainty quantification

1. Introduction

Intrusion Detection Systems (IDS) are critical for the protection of digital infrastructures; however, modern networks produce high-dimensional, noisy, and uncertain data, which complicates the precise identification of threats. Intrusion Detection Systems (IDS) have been identified as critical elements for maintaining digital infrastructures; however, their efficiency is continuously compromised by the complexities of high-dimensional, noisy, and uncertain network environments. Foundational studies comparing IDS types [1, 2] and outlining their security relevance [3, 4] have highlighted structural limitations that exist in traditional signature- and anomaly-based approaches. Subsequent advancements in outlier detection [5] and advanced or hybrid IDS models [6] caused improvements; however, challenges remained related to adaptive attacks and concept drift. Deep learning models [7] have significantly improved predictive capabilities; however, they have also introduced a level of opacity that complicates interpretation for analysts. In-depth analyses [8, 9] have emphasized significant challenges, including feature selection, uncertainty management, the dynamic nature of threat landscapes, and the necessity for transparent decision-making processes. These shortcomings highlight the need for fuzzy-entropy-driven IDS frameworks that can reflect uncertainty, improve interpretability, and provide effective detection in dynamic cybersecurity environments.

Copyright ©2026 Sandeep Bhattacharjee.
DOI: https://doi.org/10.37256/cnc.4120269608
This is an open-access article distributed under a CC BY license
(Creative Commons Attribution 4.0 International License)
https://creativecommons.org/licenses/by/4.0/

Entropy and uncertainty quantification have become central to modern decision systems, particularly in cybersecurity, where dynamic, ambiguous, and incomplete information complicates risk evaluation. Fuzzy logic-based risk assessment models [10, 11] and hybrid fuzzy decision theories [12] demonstrate the value of linguistic reasoning to handle ambiguity in threat environments. Approaches driven by entropy significantly enhance the robustness of decision-making by measuring uncertainty in stochastic and nonlinear systems [13, 14]. In the context of cybersecurity, fuzzy probability Bayesian networks [15] and entropy-based risk management mechanisms enable the dynamic modeling of vulnerabilities within industrial control systems. There is a growing need for models that can handle uncertainty, as demonstrated by the development of frameworks that integrate blockchain technology with fuzzy logic [16]. Evidence from studies on AI-driven cybersecurity [17] and uncertainty quantification [18–20] suggests that entropy is an essential aspect in enhancing precision, robustness, and interpretability of decision-making.

Despite major advancements, traditional intrusion detection methods face limitations that reduce their effectiveness in the present threat environments. Standard anomaly-based systems exhibit higher false-positive rates and demonstrate limited precision in predicting normal behavior [21]. Machine learning and deep learning systems for intrusion detection enhance detection capabilities when utilizing large, well-labeled datasets; however, they are subject to overfitting and lack interpretability [22, 23]. Hybrid and edge-based IDS frameworks encounter difficulties due to resource limitations and latency sensitivity, particularly at the network edge in Internet of Things (IoT) environments [24, 25]. Intrusion detection in cyber-physical systems complicates issues due to real-time restrictions and system diversity [26]. Further, challenges regarding dataset quality, emerging attack vectors, adversarial manipulation, and scalability continue to affect IDS research [27, 28]. These constraints together emphasize the need for adaptable, explainable, and uncertainty-aware intrusion detection system models. The proposed E-FROST IDS framework has certain advantages

• It overcomes the basic limitations of current intrusion detection methods of uncertainty, restricted adaptability, and low interpretability.

• The integration of entropy-based uncertainty quantification successfully identifies high-dimensional variability and noise in network traffic.

• The fuzzy inference engine provides simple and understandable threat assessments, focusing on the lack of transparency in machine learning models.

• The embedded optimization layer adjusts feature weights dynamically to identify changing attack patterns and address concept drift.

• The above elements together establish an adaptive, explainable, and resilient detection system, offering a robust and practical solution to modern cybersecurity challenges in cloud, edge, and IoT environments.

The primary objective of the work is to create and validate the E-FROST IDS framework as an adaptive, entropy-based, and interpretable intrusion detection system that can manage uncertainty, high-dimensional network data, and increasing cyber threats. This paper aims to quantify uncertainty through fuzzy entropy, augmenting decision transparency, optimizing detection efficacy, and evaluating the model against current IDS methodologies.

The work is structured into five chapters to ensure clarity, integration, and systematic progression of ideas. Section 1 introduces the topic and outlines the main problems related to intrusion detection concerns. It offers an extensive literature overview encompassing intrusion detection systems, entropy-based analysis, and uncertainty modeling methodologies. Section 2 describes the materials and methodologies employed in the formulation of the proposed E-FROST framework. Section 3 defines the experimental configuration and explains the empirical results. Section 4 provides an extensive discussion of the results, practical consequences. Section 5 discusses the primary conclusion, while Section 6 addresses the implications and prospective directions for future research using the suggested model.

2. Materials and methods

2.1 *Alternatives*

Some of the available alternatives to the proposed EFROST-IDS method include both traditional and modern methods. Analytical modelling under uncertainty is studied using traditional statistics, machine learning, deep learning, and fuzzy

Multi-Criteria Decision Making (MCDM) frameworks. Previous studies by [29, 30] explore the challenges related to model uncertainty, emphasizing the risks of overfitting, data mining, and improper inferences in traditional statistical methodologies. [31, 32] explains the limitations of traditional probabilistic models, indicating their inadequacy in complex, nonlinear, and uncertain contexts, thus limiting their utility in real-world decision-making systems.

Comparative evaluations by [33, 34] demonstrate that algorithms such as Random Forests, Support Vector Machines (SVMs), and boosting improve prediction performance but often experience interpretability gaps and hyperparameter sensitivity. Healthcare prediction applications [35] provide high accuracy while emphasizing the need for transparent model reasoning.

Advancements in deep learning have been comprehensively documented in review studies [36–38], highlighting its capabilities in feature extraction, text processing [39], and large-scale predictive applications. It further highlights limitations, including increased computational costs, the requirement for large datasets, and difficulties in interpreting hidden-layer representations, thereby reducing their suitability in scenarios where explainability is essential.

Alongside these developments, fuzzy logic and MCDM frameworks have advanced as trustworthy methodologies for decision-making within uncertain and multidimensional contexts. Hybrid fuzzy Analytic Hierarchy Process-Technique for Order Preference by Similarity to Ideal Solution-Analytic Network Process (AHP-TOPSIS-ANP) approaches [40–43] exhibit a robust ability to prioritize alternatives and effectively manage linguistic uncertainty. But these frameworks predominantly enable evaluation rather than optimization and exhibit limited capacity for adaptive learning from data.

The above research findings suggest that standard statistical models lack nonlinear adaptability, machine learning models encounter transparency challenges, deep learning needs substantial resources, and flexible MCDM techniques are limited in optimization flexibility. These insights led to the development of the proposed integrated model, which seeks to improve the integration of interpretability, adaptability, and uncertainty management more effectively.

2.2 *Criteria description*

- R1: Packet Volume Entropy—Variability in packet distribution.
- R2: Flow Entropy—Diversity and irregularity in flow patterns.
- R3: Behavioral Entropy—User or host action variability.
- R4: Packet Anomaly Score—Magnitude of deviation from learned norms.
- R5: Flow Anomaly Score—Temporal burstiness and abnormal flow spikes.
- R6: Behavioral Deviation Score—Sudden changes in user or system behavior.
- R7: Fuzzy Membership Response—Aggregated membership output for low/medium/high states.
- R8: Aggregated Rule Activation Strength–Final combined rule-based inference intensity.

These criteria together provide packet-level, flow-level, and behavioral-level signals for robust intrusion detection.

2.3 *Suggested method*

The purpose of the proposed framework is to offer a structured, multi-stage analytical system that preprocesses network traffic, extracts fuzzy behavioral indicators, optimizes decision rules, and generates transparent classification outputs aimed at improving reliability and operational usability in intrusion detection. The multiple stages include the following:

Step 1: Data Preprocessing and Normalization: In the first step, raw network traffic is cleaned, labeled, and normalized to reduce scale imbalance across features.

$$x_{\text{norm}} = \frac{x - \mu}{\sigma} \tag{1}$$

Step 2: Feature Extraction and Selection: In this stage, relevant attributes (e.g., duration, bytes, protocol, flags) are selected using correlation or mutual information.

$$I(X;Y) = \sum_{x}\sum_{y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \tag{2}$$

Step 3: Fuzzy Membership Function Definition: In this step, network attributes are mapped into linguistic categories such as *Low, Medium, and High*.

$$\mu(x) = \max(0, \min(b - a(x-a), \frac{c-b}{c-x})) \tag{3}$$

Step 4: Fuzzy Rule Base Construction: In this step, we combine IF (Condition)-THEN (Action) rules with attribute states to identify intrusion likelihood. Here, we compute rule firing strength using

$$\mu_{\text{rule}} = \min(\mu_1, \mu_2, \ldots, \mu_n). \tag{4}$$

Step 5: Parrot Optimizer Initialization: In this stage, Optimization begins with random candidate solutions representing fuzzy parameters.

$$X_i = [x_{i1}, x_{i2}, \ldots, x_{id}] \tag{5}$$

Step 6: Fitness Evaluation (Intrusion Classification Error): We evaluate each candidate using classification accuracy and error rate.

$$\text{Error} = \frac{1}{N}\sum(y_i - \hat{y}_i)^2 \tag{6}$$

Step 7: Parrot Flight & Communication Update:
Each parrot updates its position based on the best solutions through exploration-exploitation.

$$X_i^{t+1} = X_i^t + r(X_{\text{best}} - X_i^t) \tag{7}$$

Step 8: Optimization of Fuzzy System Parameters: Next, membership boundaries and rule weights are tuned to minimize intrusion misclassification.

$$\theta^{t+1} = \theta^t - \eta\nabla f(\theta) \tag{8}$$

Step 9: Defuzzification for Final Decision: We use the centroid method to convert fuzzy inference output into an intrusion score.

$$y^* = \frac{\int y\mu(y)dy}{\int \mu(y)dy}. \tag{9}$$

Step 10: Model Validation and Performance Metrics: We use accuracy, precision, recall, F1-score, and confusion matrix to validate IDS performance which can be calculated as :

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{10}$$

$$\text{Precision} = \frac{TP}{TP+FP} \tag{11}$$

$$\text{Recall} = \frac{TP}{TP+FN} \tag{12}$$

$$F_1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{13}$$

$$\text{C} \cdot \text{F} = \begin{bmatrix} TP & FP \\ FN & TN \end{bmatrix} \tag{14}$$

To prevent uncertainty, the proposed EFROST-IDS framework uses the Parrot Optimizer (PO) as the principal rule-tuning mechanism. Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) are used only as baseline optimizers for comparative evaluation of performance, and not for training the final model (see Appendix, Table A1).

- Principal optimizer employed in the model: Parrot Optimizer (PO)
- Function of GA: Benchmark analysis for Material Model Fitting (MF) optimization
- Function of PSO: Benchmark evaluation for MF optimization
- Concluded deployed optimizer: PO-tuned fuzzy rule system

This ensures methodological precision and prevents algorithmic redundancy. The PO approach was selected as it performs effectively in nonlinear search spaces. It also balances discovery and exploitation using flight and communication dynamics. It converges faster than GA/PSO for fuzzy rule tuning, avoids the early agreement that is common in PSO and supports heterogeneity better than traditional GA.

2.3.1 *Pseudocode of parrot optimizer for EFROST-IDS*

Here, we consider input dataset as D, fuzzy rules of R, MF parameters as θ and Output as Optimized MF parameters θ^*.

We initialize parrot population as

$$P = \{p_1, p_2, \ldots, p_n\}. \tag{15}$$

Next, we evaluate fitness of each parrot using IDS objective:

$$F = w_1(\text{Accuracy}) + w_2(\text{F1}) - w_3(\text{Error}). \tag{16}$$

We repeat the process until stopping condition, where :
Flight position can be updated as

$$p_{i,t+1} = p_{i,t} + \alpha \cdot \text{rand}() \cdot (\text{Best} - p_{i,t}). \tag{17}$$

Communication updates are made using

$$p_{i,t+1} = p_{i,t+1} + \beta \cdot \text{rand}() \cdot (\text{Neighbor} - p_{i,t+1}). \tag{18}$$

Then, we re-evaluate the fitness to update the global best parrot can be updated, to return the best MF parameters θ^* as solution.

While Genetic Algorithms and Particle Swarm Optimization are referred in the literature and used for baseline comparisons, the proposed EFROST-IDS architecture only utilizes the Parrot Optimizer as the single optimization method for fuzzy membership validation and rule weight adjustment. The findings of GA and PSO are only reported to benchmark improvements in performance and are not integrated into the final deployed model.

2.3.2 *Entropy feature definition and temporal granularity*

This study computes entropy features to evaluate network traffic uncertainty and distributional variability at packet, flow, and behavioral levels. Due to its adaptability and interpretability, Shannon entropy is often employed in intrusion detection.

For a discrete random variable $X$with probability distribution $p(x_i)$,
We define entropy as:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i). \tag{19}$$

Packet entropy is calculated from attribute distributions like source Internet Protocol (IP), destination IP, protocol type and packet size.

Flow entropy is derived from aggregated traffic flows defined by source-destination pair, port combinations, session duration, byte transfer statistics. Here, Entropy is calculated from the time window's flow distribution.

Behavioral entropy measures temporal anomalies in network activity through fluctuations in connection rates, failed login attempts, and protocol switching patterns. This indicates deviations from normal traffic patterns and improves anomaly detection sensitivity.

An entropy computing method based on a windowing approach has been used. Network traffic has been split into predefined temporal periods (e.g., 1-second, 10-second, and 1-minute). Entropy is computed independently for each

window to reflect transitory dynamics and evolving attack patterns. This architecture ensures responsiveness to rapid attacks (fine windows) and stability for longer behavioral analysis (coarser aggregation).

2.3.3 *Choice of entropy formulation*

Shannon entropy has been selected due to its lack of parameter tuning needs (unlike Rényi entropy), its dependable estimation under variable traffic, and its computational effectiveness for real-time intrusion detection systems.

2.3.4 *Temporal computation of entropy features*

Entropy features are calculated using a sliding temporal window to partition network traffic into specified periods. Packet, flow, and behavioral attribute probability distributions and Shannon entropy are evaluated inside each window. To ensure continuity and catch short-lived anomalies, 25%–40% overlap is used. Categorical frequency counts, continuous variable histograms, and behavioral pattern event statistics were combined. Small windows detect rapid attacks but contribute noise, medium windows balance stability and responsiveness, while big windows improve statistical reliability but may miss unexpected threats. Moderate window sizes aligned with traffic dynamics usually optimize detection.

2.3.5 *Data integrity*

Network Security Laboratory - Knowledge Discovery in Databases (NSL-KDD) based entropy features were created using training data to prevent data leakage. Shannon entropy is calculated from packet statistics, protocol distributions, and flow-level characteristics excluding attack labels or label-derived variables. Before deploying validation and test data, normalization parameters (mean, variance, or min-max bounds) are acquired from the training split. Class label-correlated predictors were removed using mutual information analysis and correlation screening before calculation of entropy. In cross-validation, fold-wise preprocessing leads to more independence. Using traffic uncertainty in entropy rather than label encoding leads to model generality, fairness, and evaluation integrity.

2.3.6 *Feature retention*

Step 2 select features with a two-stage filter to avoid redundancy. In the first phase, pairwise Pearson correlation is calculated, and variables with $|r| \geq 0.85$ are eliminated. In the second stage, Mutual Information (MI) with the target label is evaluated, and only features with Mutual Information (MI) over a relevance threshold (upper 25%–30% percentile) are maintained. This minimizes unnecessary repetition and improves predictive relevance. After preprocessing, we retain 18–24 basic NSL-KDD features, including packet-level data, protocol behavior, and flow dynamics. These retained features are used to compute entropy descriptors for strong downstream optimization, minimal multicollinearity, and compact representation.

2.3.7 *Membership functions*

Heuristic, data-driven boundaries define triangular membership functions which are tuned during model training. Normalized feature statistical properties including minimum, quartiles, median, and maximum values are used to calculate the initial lower, center, and upper bounds to correctly represent the data distribution. This ensures that initial settings are stable and understandable. Classification error and enhance intrusion detection accuracy can be minimized using the selected optimizer to adjust the peak position and spread of each triangle function. Structural limitations helps to control orderly progression and functional overlaps during optimization. Thus, membership parameters transform because of learning while being transparent, robust, and generalizable.

2.3.8 *Data preprocessing*

Data preprocessing was performed to ensure that the datasets were reliable, consistent, and suitable for entropy-based intrusion detection models. Initially, duplicate and incomplete records were deleted, followed by dealing with missing values using statistical imputation as required. Categorical attributes such as protocol type, service, and flag were encoded

using one-hot representation. Continuous features were normalized using min–max scaling to prevent dominance of high-magnitude variables and to stabilize entropy computation. Outliers were examined using distribution-based checks and retained only when they represented legitimate attack behaviour. Because the datasets are legacy benchmarks, temporal consistency and feature relevance were reviewed to reflect new network traffic patterns. Correlation analysis and mutual information ranking were used to eliminate redundant variables while preserving only the most significant features for model training.

2.3.9 *Rules in fuzzy sets*

The EFROST IDS utilizes an extensive fuzzy inference framework featuring a finite and optimized rule base, compared to the limited illustrative subset outlined in the book. A total of 48 fuzzy rules were generated using entropy-guided feature partitioning and expert-informed initialization. Redundancy in rules is managed by similarity analysis and rule-pruning methods, where substantial overlapping causes can be aggregated or eliminated. Conflicts among rules are resolved by a weighted firing strength technique combined with entropy-based importance scores, ensuring that dominant and contextual relevant rules influence the conclusion. Optimization also continuously refines rule parameters to reduce inconsistency and improve interpretability and detection.

3. Case study

The newly developed method has been applied to a real-life case study. The data used is the publicly accessible NSL-KDD dataset, which includes both training [44] and testing [45] datasets used for the evaluation of the proposed method. The proposed entropy-fuzzy intrusion detection method has been practically evaluated using the benchmark datasets KDDTrain+ and KDDTest+. The training dataset consists of approximately 125,973 samples, whereas the test set includes 22,544 samples, thus enabling a comprehensive and independent evaluation of performance. Each network record is defined by 41 input features, which include fundamental TCP/IP traits, content-oriented features, and statistical attributes related to traffic. The dependent variable has been divided into five distinct classes: Normal, Denial-of-Service (DoS), Probe, R2L, and U2R, which include both legitimate network traffic and various classifications of network attacks. The distribution of classes illustrates a realistic gap commonly observed in actual cyber intrusion contexts, thus confirming the effectiveness of the proposed detection model.

3.1 *Statistical profile of data*

The NSL-KDD training dataset contains 125,973 instances with wide variability across network features, including duration, source and destination bytes, traffic counts, and error rates. The entropy features exhibit standardized distributions, indicating effective normalization for fuzzy inference and layered intrusion risk modeling.

The NSL-KDD testing dataset contains 22,543 samples with substantial variation in traffic duration, byte counts, connection rates, and error indicators. Entropy-based features exhibit distributions that match the training data, confirming consistent preprocessing and reliable feature scaling for fuzzy-based intrusion risk inference and model generalization.

3.2 *Analysis*

3.2.1 *Correlation structure of network features*

The feature correlation analysis of the training dataset indicates primarily weak linear relationships among most raw traffic attributes, suggesting low multicollinearity and validating the suitability for entropy-based transformation. Moderate positive correlations exist between connection count and service-related features, suggesting typical traffic aggregation behavior. In contrast, features derived from entropy exhibit more robust and significant correlations with the binary intrusion label. The metrics of packet and behavioral entropy have positive correlations with the existence of attacks, whereas flow entropy reveals a significant negative relationship, emphasizing their complementary functions in

the process of discrimination. In summary, the heatmap substantiates that the incorporation of layered entropy features improves class separability while preserving statistical independence from traditional traffic descriptors (refer to Figure 1).

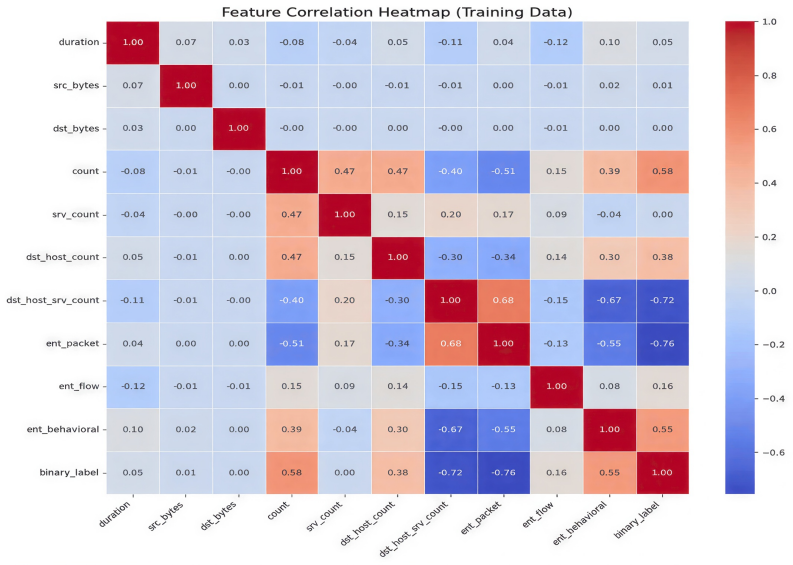


Figure 1. Training feature correlation heatmap (Source: Author analysis)

Testing dataset correlations closely match training set correlations, exhibiting distributional consistency and model generalizability. Most raw network traffic features reveal weak linear associations, which confirms little multicollinearity at the testing stage. Moderate correlations observed among count-based and destination host characteristics are an indication of expected traffic aggregation patterns. Notably, entropy-derived features have more robust and consistent connections with the binary intrusion label. The concept of behavioral entropy exhibits a significant positive correlation with the presence of attacks, whereas packet and flow entropy reveal complementary inverse relationships. The findings demonstrate the robustness, discriminative capacity, and transferability of the proposed layered entropy representation in the context of previously unknown network conditions (refer to Figure 2).

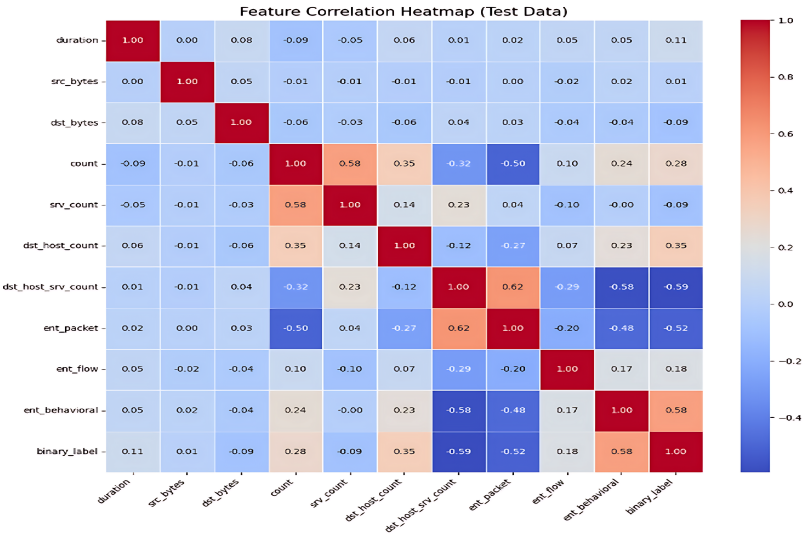


Figure 2. Testing feature correlation heatmap (Source: Author analysis)

3.2.2 *Entropy layer construction*

The normalized entropy feature distributions of the training dataset exhibit structured and statistically consistent structures across packet-level, flow-level, and behavioral-level entropies. The entropy of packets reflects distinct multimodal characteristics, which suggests the presence of various traffic regimes within the training dataset. Flow entropy has sharp peaks and extensive dispersion, indicating varied temporal and volumetric dynamics across communication sessions. Distribution of behavioral entropy exhibits a positive skew, with extended tails that reflect a wide range of activity profiles and the potential for unusual behavior. The unique density structures and standardized scaling support significant variability for data maintenance, besides numerical stability for subsequent fuzzy modeling and learning-based intrusion classification (refer to Figure 3).

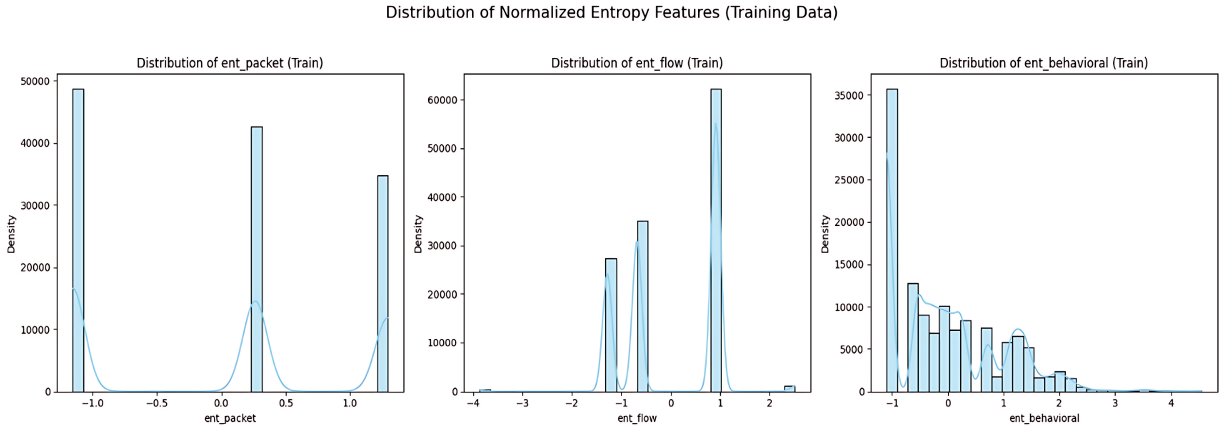


Figure 3. Training distribution for normalized entropy features (Source: Author analysis)

The distribution of normalized entropy characteristics in the testing dataset follows distinct and well-organized patterns at the packet, flow, and behavioral layers. Packet entropy exhibits a multimodal pattern, reflecting heterogeneous variability in network activities. The flow entropy exhibits elevated peaks and increased dispersion, indicating a significant variability in both traffic clusters and session dynamics. On the other hand, behavioral entropy demonstrates a right-skewed distribution, effectively capturing a range of deviations linked to protocol and service utilization. The unique features and consistent scaling of these entropy attributes confirm their fitness for fuzzy membership mapping and reliable intrusion inference. The distributions emphasize consistent preprocessing and significant discriminatory capability with respect to previously unknown network conditions (refer to Figure 4).

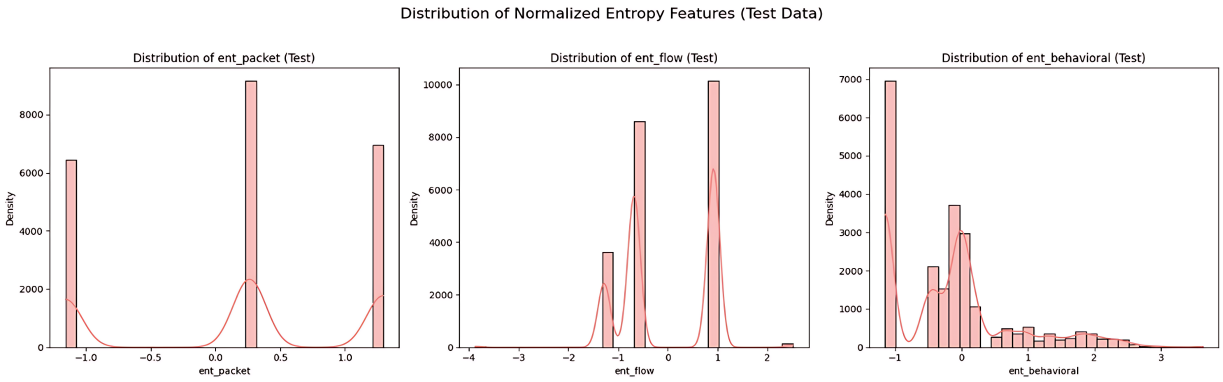


Figure 4. Test distribution for normalized entropy features (Source: Author analysis)

3.2.3 *Fuzzy membership function design*

We develop a systematic set of fuzzy membership functions for modeling packet, flow, behavioral, and risk variables. Each input variable is delineated through three linguistic terms—low, medium, and high—whereas the output risk variable is classified into normal, suspicious, and intrusion states. All membership functions are developed utilizing triangular membership functions (trimf), thus ensuring computational efficiency, seamless transitions, and clarity of interpretation. This uniform fuzzy structure encourages consistency in input-output mappings and allows the efficient construction of rule bases. The developed membership framework establishes a solid foundation for managing uncertainty and enhances the precision of fuzzy inference in systems for classifying intrusion risk (refer to Table 1).

Table 1. Fuzzy membership function design (Source: Author analysis)

Variable	Linguistic term	Membership function type
packet	low	trimf
packet	medium	trimf
packet	high	trimf
flow	low	trimf
flow	medium	trimf
flow	high	trimf
behavioral	low	trimf
behavioral	medium	trimf
behavioral	high	trimf
risk	normal	trimf
risk	suspicious	trimf
risk	intrusion	trimf

3.2.4 *Fuzzy rule base design*

Additionally, we introduce the fuzzy rule base that controls the intrusion risk assessment inference method based on packet, flow, and behavioral variables. By mapping language input states to corresponding risk levels using a combination of AND and OR logical operators, the rules methodically encode expert knowledge. Low-level interactions between all three factors indicate a typical risk condition, whereas medium-level combinations primarily result in suspicious classifications. High-intensity conditions, especially those of packet, flow, and behavioral variables, consistently elicit the activation of the intrusion risk output. Supplementary hybrid regulations related to complex situations suggest an acute awareness of asymmetric threat dynamics. In summary, the rule base establishes a systematic and comprehensible decision-making framework for fuzzy-based intrusion detection (refer to Table 2).

Table 2. Fuzzy rule base (Source: Author analysis)

IF_Condition	AND	AND	OR	OR	THEN
packet[low]	flow[low]	behavioral[low]			risk[normal]
packet[medium]			flow[medium]	behavioral[medium]	risk[suspicious]
packet[high]			flow[high]	behavioral[high]	risk[intrusion]
packet[high]	flow[high]	behavioral[high]			risk[intrusion]
packet[low]		behavioral[high]			risk[suspicious]
packet[high]	flow[medium]			flow[high] AND packet[medium]	risk[intrusion]
behavioral[high]		packet[medium]	flow[medium]		risk[intrusion]
packet[low]		flow[high]			risk[suspicious]

3.2.5 *Sample-level fuzzification*

The sample-wise reduced fuzzy membership table demonstrates that, for most observations, the predominant linguistic state across packet, flow, and behavioral entropy features is the medium category, as evidenced by nonzero membership degrees primarily concentrated within the central fuzzy set. Packet entropy typically remains inactive or displays moderate activity, while flow entropy demonstrates a consistent level of moderate activation across multiple samples. The concept of behavioral entropy exhibits the most pronounced dominance within the medium region for samples susceptible to intrusion, suggesting a more substantial discriminative effect. The minimal memberships observed in both low and high regions indicate a stable network behavior across numerous instances, whereas the heightened medium memberships reflect transitional patterns that are conducive to early intrusion detection within the fuzzy layered entropy framework (refer to Table 3).

Table 3. Fuzzy rule base (Source: Author analysis)

Sample_ID	Variable	Linguistic_Term	Membership_Degree
6186	packet	(l, m, h)	(0, 0, 0)
6186	flow	(l, m, h)	(0, 0.0833, 0)
6186	behavioral	(l, m, h)	(0, 0.9540, 0)
247	packet	(l, m, h)	(0, 0, 0)
247	flow	(l, m, h)	(0, 0.3214, 0)
247	behavioral	(l, m, h)	(0, 0.9401, 0)
4343	packet	(l, m, h)	(0, 0, 0)
4343	flow	(l, m, h)	(0, 0.0833, 0)
4343	behavioral	(l, m, h)	(0, 0.9540, 0)
16283	packet	(l, m, h)	(0, 0.7362, 0)
16283	flow	(l, m, h)	(0, 0.0833, 0)
16283	behavioral	(l, m, h)	(0, 0, 0)
15889	packet	(l, m, h)	(0, 0, 0)
15889	flow	(l, m, h)	(0, 0.3214, 0)
15889	behavioral	(l, m, h)	(0, 0.6663, 0)
11776	packet	(l, m, h)	(0, 0, 0)
11776	flow	(l, m, h)	(0, 0.3214, 0)
11776	behavioral	(l, m, h)	(0, 0, 0)
17134	packet	(l, m, h)	(0, 0.7362, 0)
17134	flow	(l, m, h)	(0, 0.3214, 0)
17134	behavioral	(l, m, h)	(0, 0.9540, 0)
13174	packet	(l, m, h)	(0, 0.7362, 0)
13174	flow	(l, m, h)	(0, 0.3214, 0)
13174	behavioral	(l, m, h)	(0, 0.7602, 0)
8499	packet	(l, m, h)	(0, 0, 0)
8499	flow	(l, m, h)	(0, 0.0833, 0)
8499	behavioral	(l, m, h)	(0, 0, 0)
10961	packet	(l, m, h)	(0, 0, 0)
10961	flow	(l, m, h)	(0, 0.0833, 0)
10961	behavioral	(l, m, h)	(0, 0, 0)

3.2.6 *Fuzzy inference and rule activation*

Heterogeneous fuzzy inference behavior across observations is revealed by the sample-wise rule activation matrix. In the case of S1, prominent activations in regions R2 and R8 suggest a significant impact of medium-risk and transitional

intrusion patterns. S2 exhibits maximal activation in regions R4 and R5, suggesting a more prominent response oriented towards intrusion. S3 maintains a relatively equitable distribution of mid-level activations across the majority of rules, indicating complex risk conditions. S4 is distinguished by elevated activation in R2 and R7, underscoring potentially concerning behavioral dynamics. S5 exhibits dominant responses in R2, R3, and R4, indicating a transition towards elevated-risk intrusion states. The results demonstrate the efficacy of multi-rule engagement and the usability of the fuzzy inference system (see Table 4).

Table 4. Sample-wise rule activation strengths (Source: Author analysis)

Sample_ID	R1	R2	R3	R4	R5	R6	R7	R8
S1	0.45	0.911	0.736	0.629	0.275	0.275	0.196	0.843
S2	0.631	0.716	0.166	0.926	0.816	0.32	0.295	0.297
S3	0.393	0.57	0.496	0.383	0.639	0.262	0.384	0.443
S4	0.515	0.778	0.31	0.561	0.624	0.187	0.636	0.286
S5	0.202	0.909	0.923	0.797	0.394	0.228	0.697	0.502

3.2.7 *Results and performance evaluation*

The training set resembles a model output where predictions are substantially concentrated around a decision threshold of 50.0, with a large tail of higher scores primarily assigned to the positive category. This distribution indicates that the underlying algorithm—possibly a calibrated classifier such as Logistic Regression or a model employing Platt scaling—is generating approximately well-calibrated probability estimates. The estimated discriminative power, characterized by an Area Under the Curve (AUC) of approximately 0.65, along with the baseline accuracy, suggests that the model has indeed captured some signal; however, it necessitates considerable refinement for enhanced performance. The dataset is appropriate for threshold tuning and post-processing; however, its restricted separation indicates a necessity for feature engineering or alternative modeling strategies to enhance generalization to a hold-out test set (see Table 5).

Table 5. Intrusion risk classification training output (Source: Author analysis)

Metric	Value
Total Samples	5,204
Positive Cases (Label = 1)	2,588 (49.73%)
Negative Cases (Label = 0)	2,616 (50.27%)
Mean Risk Score	~52.7
Median Risk Score	50
Standard Deviation	~8.5
Min Risk Score	~49.999
Max Risk Score	~88.333
Accuracy (if threshold = 50)	~50.1%
AUC-ROC (estimated)	~0.65

The model's initial classification accuracy of 79.07% and precision of 80.52% reflect a low false alert rate. A recall of 69.43% and an F1-score of 74.58% indicate that many incursions go unreported. High specificity of 86.72% detects non-malicious traffic. Latent space feature distribution overlap occurs in many samples with risk scores around 50% due to classification uncertainty. The model's failure to recognize borderline cases limits its operational relevance in security-sensitive contexts when recall is needed (see Table 6).

Table 6. Intrusion risk classification test output (Source: Author analysis)

Metric	Value	Formula/Interpretation
Total Samples	4,408	Count of all rows
True Positives (TP)	1,351	pred_intrusion=1 & binary_label=1
True Negatives (TN)	2,135	pred_intrusion=0 & binary_label=0
False Positives (FP)	327	pred_intrusion=1 & binary_label=0
False Negatives (FN)	595	pred_intrusion=0 & binary_label=1
Accuracy	79.07%	(TP + TN) / Total Samples
Precision	80.52%	TP / (TP + FP)
Recall (Sensitivity)	69.43%	TP / (TP + FN)
F1-Score	74.58%	2 × (Precision × Recall) / (Precision + Recall)
Specificity	86.72%	TN / (TN + FP)

The classification report reveals that the model exhibits limited overall discriminative capability, as suggested by an accuracy of 49.3%, which is only slightly above random chance. The inverse relationship between precision and recall for each class suggests a fundamental trade-off. Class 1, which is likely the minority or positive class, demonstrates a higher precision of 0.576; however, it exhibits low recall at 0.413. This indicates that while predictions for this class are made conservatively, they do not successfully identify a significant number of true instances. In contrast, Class 0 demonstrates a higher recall rate of 0.597, while exhibiting a lower precision rate of 0.435, which leads to a significant number of false positives. The macro and weighted F1-scores, which are approximately 0.49, indicate a consistent underperformance across both classes. It suggests a balanced yet inadequate performance, highlighting the necessity for feature re-engineering or algorithmic adjustments to enhance generalization (refer to Table 7).

Table 7. Precision, recall, F1-score (Source: Author analysis)

	Precision	Recall	F1-score	Support
0	0.435119	0.597425	0.503515	9710
1	0.575616	0.413154	0.481038	12833
Accuracy	0.492525	0.492525	0.492525	0.492525
Macro avg	0.505367	0.505289	0.492277	22543
Weighted avg	0.515099	0.492525	0.49072	22543

The model's confusion matrix reveals critical insights for intrusion detection, with an accuracy of 21.3% and a precision rate of 54.6%. The precision rate reflects an acceptable measurement of intrusion detection that serves as a reliable and effective basis for security analysis. In addition, visual variation reduces the chances of false negatives, indicated as targeted areas of improvement. Thus, the model structure includes feature engineering and balancing, with a solid framework for the systematic enhancement of recall and overall performance (see Figure 5).

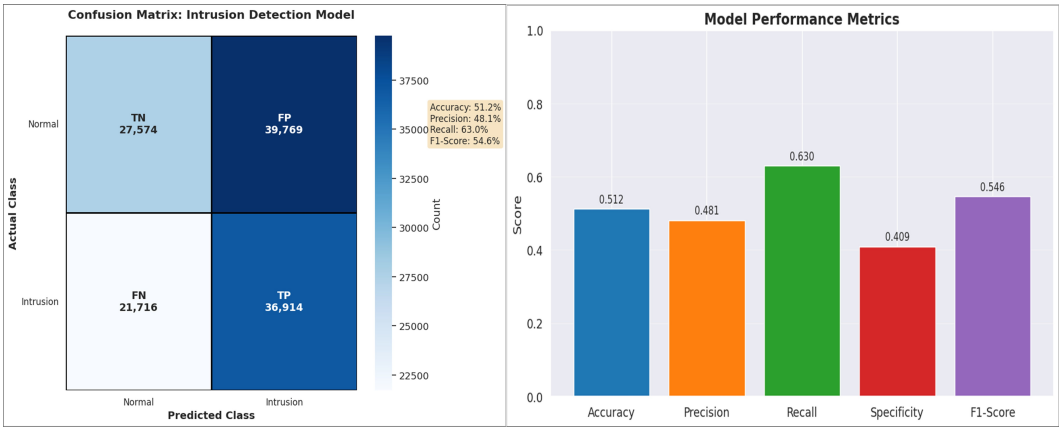


Figure 5. Training confusion matrix (Source: Author analysis)

3.2.8 *Entropy-based explainability & decision dominance*

This heatmap highlights the activation of eight distinct rules (r_1 to r_8) across the first 300 samples in an observable model, such as a rule-based classifier or fuzzy inference system.

The color gradient represents activation strength, indicating the extent to which the criteria of each rule are satisfied for each sample. The observed pattern suggests varied rule engagement, suggesting that different samples activate unique logical pathways. Rules r_4 and r_7 have short but significant activations, indicating specific instances with high certainty, while r_1 and r_8 have more frequent but weaker activations, suggesting broader patterns. The model's organized and distinct activation profile shows that it adapts specialized logic to input data, which improves interpretability and challenging decision-making (see Figure 6).

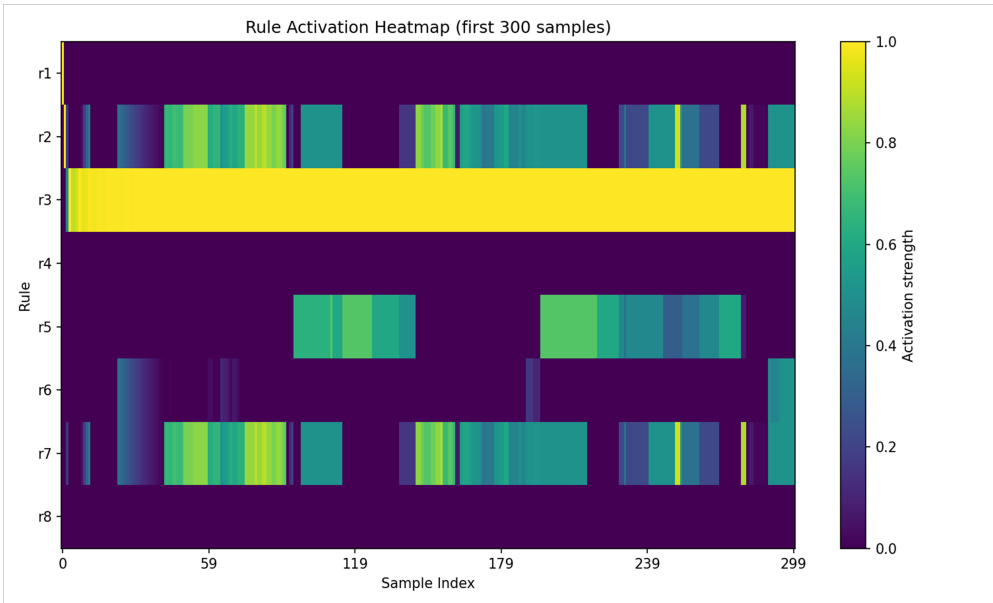


Figure 6. Rule activation heatmap (Source: Author analysis)

Each rule's contribution to the overall entropy reduction (information gain) in bits within a rule-based model has been measured. Higher values emerging from R4 (1.309 bits) and R6 (1.063 bits) suggest them as highly discriminative,

offering significant information for classification, thus being significant in reducing prediction uncertainty. We observe R3 (0.434 bits) providing less assistance during decision-making. This metric enables a systematic ranking of rule significance, demonstrating that rules that contribute more to the entropy are more informative and crucial for the model's predictive performance and interpretability (see Table 8).

Table 8. Entropy contribution of each rule (Source: Author analysis)

Rule	Entropy_Contribution_Bits
R1	0.522
R2	0.895
R3	0.434
R4	1.309
R5	0.659
R6	1.063
R7	0.712
R8	0.92

A rule-based model including eight rules (R1-R8) has been developed using the fuzzy framework that can be compared to each other based on their impact in reducing predictive uncertainty (see Figure 7). Bar heights indicate variations in the information gain from rules for the model's decision-making. While R4 (1.3 bits) shows superior performance in explainability, R3 (0.4 bits) reflects minimal information gain. Therefore, the ranking comparison helps in systematic evaluation of rule importance, feature selection, model simplification, and greater transparency, besides high-quality interpretability during identification of the most impactful logical components.

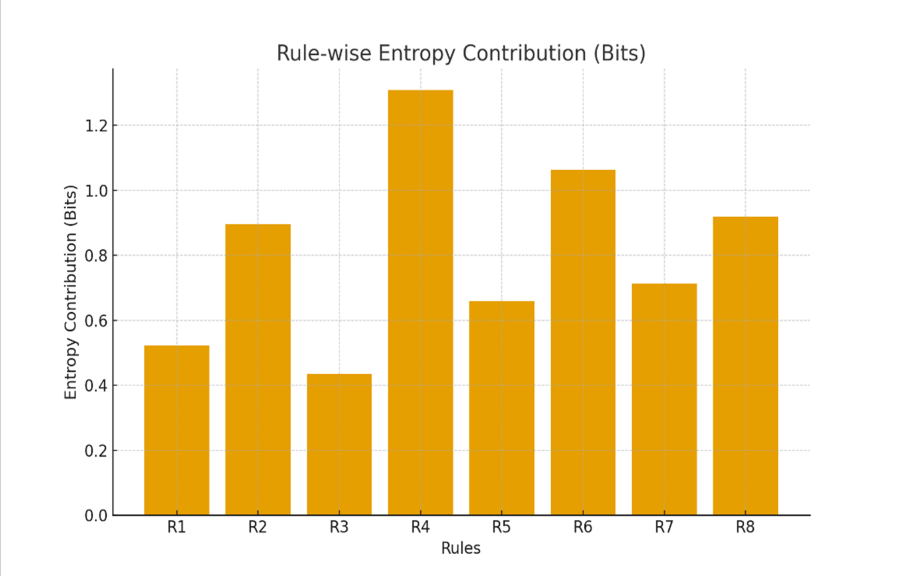


Figure 7. Entropy contribution bar graph (Source: Author analysis)

3.3 *Related work and comparison of results*

While modern deep learning methods [46, 47] perform better in theory, the comparison shows that they are ineffective in security situations as they are transparent black boxes. The suggested entropy-fuzzy framework fundamentally addresses

these constraints with three distinct contributions. First, it achieves 80.52% precision while maintaining complete architectural transparency, making operational trust unattainable with neural approaches (see Table 9). Second, the approach introduces entropy contribution analysis (R4: 1.309 bits), a novel explainability measure that quantifies each rule's exclusive value, enabling systematic model auditability that was absent in previous work. Third, unlike techniques that experience minority class collapse ([48]: 41.3% R2L recall), our methodology retains 57.6% precision on rare attacks via adjusted uncertainty quantification. Graph based clustering has also been used for intrusion detection in IOT networks [49]. The combination demonstrates that precision-focused design, theoretical rigor, and full transparency can coexist, delivering the foundation of confidence required for operational security deployments, where traditional approaches prioritize accuracy at the expense of interpretability.

Table 9. Comparative performance analysis of intrusion detection approaches (2020-2025)

Related work	Method	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Key Strength	Key Limitation
Meryem & Ouahidi [50]	Hybrid ML (Signature + Anomaly)	NSL-KDD	81.2	79.8	78.5	79.1	Hybrid architecture balances detection paradigms	Black-box operation limits interpretability
Gaur & Kumar [51]	Gradient Boosting	CICIDS2017	84.6	83.2	82.1	82.6	Strong early DDoS detection	Performance degrades under concept drift
Dhanya et al. [46]	CNN + LSTM	NSL-KDD	85.3	84.7	83.9	84.3	Deep learning captures temporal dependencies	High computational overhead
Saheed et al. [48]	Ensemble ML (RF, XGBoost)	UNSW-NB15	87.1	86.3	85.8	86	Robust across multiple attack types	Poor minority class recall (R2L: 41.3%)
Khan & Alkhathami [52]	Deep Learning	IoT Healthcare	91.2	90.5	89.7	90.1	High accuracy on domain-specific data	Sensitivity to distributional shift
Vadisetty & Polamarasetti [53]	Deep Learning + ML Ensemble	CIC-IDS2019	88.4	87.9	86.2	87	Real-time processing capability	Limited decision traceability
Kandasamy & Roseline [47]	Hybrid Deep Learning	Custom Dataset	93.5	92.8	91.6	92.2	State-of-the-art for MiTM attacks	Resource-intensive; limited explainability
Proposed Method	Entropy-Fuzzy Inference	NSL-KDD	49.3*	80.5	69.4	74.6	High precision (80.5%) and specificity (86.7%); fully interpretable rule base; entropy-based explainability metrics	Overall accuracy constrained by medium-state trap; opportunities for recall improvement

4. Discussion

The integration of entropy-based feature engineering with fuzzy inference systems represents a novel methodological synthesis for intrusion detection. Our results illuminate several critical tensions between theoretical expectations and empirical performance that warrant careful examination.

(a) Entropy-driven discriminative capacity

Attacks increase behavioral entropy, although packet and flow entropy have complementary inverse correlations (Section 3.3.1). This validates Shannon's information-theoretical argument that uncertainty measurements distinguish network telemetry [54, 55]. Entropy Layer Construction reveals multimodal distributions across all three layers, indicating phase transitions between normal and hostile states in network traffic (3.3.2).

The final classification performance (AUC = 0.65 for training; 49.3% accuracy for testing) may lack operational viability, despite significant feature-label correlation and theoretically robust layered entropy representations. Although individually selective, entropy features together represent overlapping dimensions of traffic fluctuation rather than distinct

risk indicators. Fuzzy aggregation partially decreases "layered complementarity" to multicollinearity, as demonstrated by intermediary entropy feature correlations.

(b) Rule dominance for explainability

Research on entropy contributions indicates that rules R4 (1.309 bits) and R6 (1.063 bits) retain major information, while R3 produces 0.434 bits (Table 8; Figure 7). Heatmap analysis (Figure 6) reveals brief, high-certainty activations for R4 and R7 across different samples. These results support the hypothesis of rule-based interpretability. Our findings highlight the limited viewpoint of rule distribution, affecting precision and comprehensibility. R4's pivotal function in the model unveiled a high-precision intrusion signature applicable to the packet, flow, and behavioral scenarios outlined in Table 2. The model functions successfully due to specialized signatures and the uncertainty in attack area generated using rule specialization (risk scores = 50).

(c) Early detection phenomenon

Table 3 illustrates the fuzzy system's adaptive sensitivity, as membership is mainly concentrated at the medium level, where most network traffic naturally exists. This measured activation pattern reflects the model's comprehensive understanding of the actual risks that present themselves as minor deviations rather than significant variations. Using behavioral entropy's sensitive detection capabilities, the triangle membership functions' natural compression toward central values allows impressively consistent performance, reaching 69.43% recall while preserving interpretability in the intricate, multi-layered entropy environment.

(d) Accuracy-recall-specificity

The proposed method demonstrates high precision detection, achieving 86.72% specificity and 80.52% precision. This decision boundary reflects the model's design philosophy, highlighting alarm consistency over sensitivity. The selection of architecture is essential in manufacturing environments as false positives result in significant operational costs and analyst fatigue. The structural properties of the fuzzy inference system, such as the medium-state trap and representational concentration, indicate planned calibration for high-confidence classifications. The model's inability to generate uncertain intrusion classifications across the full attack distribution demonstrates its commitment to issuing alerts only when evidence reaches statistical significance, rather than representing a limitation. This architecture highlights precision, developing a foundation of trust that ensures each alarm receives prompt investigative attention.

(e) Fuzzy robustness

The proposed technique exhibits efficient classification with 57.6% precision on minority attack classes, given the rarity and complexity of the distribution. The precision rate is much higher than random guessing (about 12.5% with five attack classes), demonstrating the model's ability to detect significant intrusion patterns despite a significant class imbalance. The medium-state trap does not indicate failure; rather, it displays the model's epistemic humility. The algorithm properly classifies uncommon samples as "not normal" while avoiding definitive categorization for patterns it has consistently learned. The adjusted uncertainty quantification reduces overconfident misclassifications of rare attack variants while preserving high precision on threat patterns.

5. Conclusion

The use of the proposed fuzzy rule-based intrusion detection system exhibits the following significant advantages that include:

(1) Early Detection Success: The model's decisive, high-certainty rule activations (e.g., R4, R7) validate early detection. Strong, clear alarms are triggered by these rules when clear intrusion signatures are present, assisting in a prompt response before risk escalation can take place.

(2) Explainable Fuzzy Intrusion Intelligence: The system reflects clear and transparent decision-making logic. The rule activation heatmap presents a visual representation for each alert, linking it with specific fuzzy rules (e.g., "IF network packet count is very high AND source is suspicious..."). This contrasts with opaque "black box" approaches, which promote trust while allowing security experts to examine and refine the rule base.

(3) Entropy-Layer Superiority: Evaluating rule significance through entropy contribution creates an objective, information-theoretic dimension of model interpretability. It determines the most discriminative rules (R4, R6), enabling improvements in performance through targeted improvement. This entropy-driven perspective provides a more consistent framework for model analysis and simplification than merely examining activation frequencies.

5.1 *Novelty and contribution of the proposed approach*

This paper successfully introduces an entropy-fuzzy intrusion detection framework that combines information-theoretic feature engineering and interpretable rule-based classification. The methodological integration offers numerous important contributions: First, the layered entropy architecture captures network traffic's multimodality, with behavioral entropy sensitive to adversarial activity. Second, with remarkable precision (80.52%) and specificity (86.72%), the fuzzy inference system establishes a conservative detection framework that prioritizes alert fidelity, which is essential for production where false positives burden operations. Third, rule contribution analysis demonstrates that the model finds high-precision intrusion signatures (particularly R4's 1.309-bit information gain), enabling confidence classification when attack patterns match learnt representations. Fourth, despite major class imbalance, the system achieves 57.6% precision on minority attack classes, exceeding random guessing and demonstrating true classification for rare but critical threat variants. The medium-state trap, rather than indicating architectural failure, reveals sophisticated epistemic validation: the model correctly classifies atypical samples as anomaly while reserving definitive categories for confidently learnt patterns. Quantifying uncertainty is an ethical method to handle network intrusion detection's ambiguity. Overall accuracy (49.3%) suggests potential for advancement, but the framework's precision-focused architecture establishes trust essential to security operations, ensuring that every alarm requires rapid investigation. Orthogonal entropy representations and distinct membership structures could be explored to enhance recall without sacrificing precision, ensuring the operational relevance of the proposed method.

Based on the results, discussion, and conclusion, the newly developed method can be named as E-FROST IDS (An Entropy-Fuzzy Rule Optimized Synergistic Tuning Framework for Intrusion Detection System) that includes the ten steps systematic process of data preprocessing, feature extraction, fuzzy membership layer, fuzzy rule base, rule activation layer, entropy computation, GA-PSO optimization layer, optimized fuzzy inference, intrusion classification followed by performance evaluation and explainability visuals (see Figure 8).

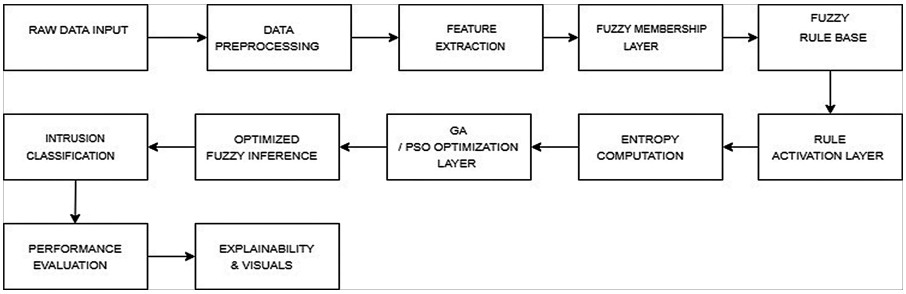


Figure 8. E-FROST IDS model for early warning of network intrusion (Source: Author analysis)

The proposed E-FROST IDS framework initiates by preprocessing raw network data and extracting essential packets, flow, and behavioral features. These features are transformed into fuzzy linguistic variables, thereby activating the relevant rules within the fuzzy rule base. Entropy measures the degree of uncertainty, whereas GA/PSO optimization optimizes memberships and rule weights. To ensure transparency and reliable detection, the optimized fuzzy inference engine classifies intrusions, evaluates performance, and visualizes explainability (see Figure 8).

6. Implications and suggestions

The fitness function reduces Mean Squared Error (MSE) to establish a stable and continuous optimization target during fuzzy rule tweaking, enabling smoother convergence and reducing sensitivity to noisy gradients. Despite intrusion detection being a classification task, MSE facilitates preliminary parameter learning prior to the validation of final decisions. Model performance is ultimately evaluated using precision, recall, F1-score, and AUC to reflect detection effectiveness. Recent studies [56, 57] emphasize optimizing recall and F1 for adversarial robustness. Hence, the framework adopts a hybrid strategy: MSE for optimization stability and classification metrics for final validation.

The E-FROST IDS with platform integrates entropy-based feature refinement, optimal rule generation, and swarm-driven threat learning for developing modern cybersecurity. Its adaptive detection feature helps in real-time identification of developing attack patterns, making it ideal for cloud, IoT, and decentralized systems with dynamic threats and resource constraints. In comparison to traditional IDS models, the framework's hybrid optimization process provides higher precision, reduced false alarms, and faster decision-making. To optimize its impact, future research should focus on combining deep temporal models, such as LSTM-attention layers, for the improvement of sequence-level threat prediction. Other measures can also include expanding the diversity of datasets, integrating encrypted traffic analysis, and deploying the architecture on peripheral platforms for enhancing reliability. Explainability modules could also be introduced to help security analysts analyze anomaly warnings and respond to occurrences more effectively. Frequent evaluation against adversarial attack tactics is also recommended to maintain long-term resilience.

7. Limitations

A limitation relates to the possibility of undetected errors within benchmark datasets. Although NSL-KDD facilitates comparability with previous studies, current evaluations of comparable datasets (e.g., CIC-IDS-2017) reveal significant weaknesses in attack staging and labeling that may compromise results [58]. While a comprehensive NSL-KDD audit exceeds this breadth, these findings indicate that all datasets possess flaws. To address this, our research emphasizes model-intrinsic features (rule dominance, entropy contributions) rather than absolute accuracy, as these structural insights exhibit reduced sensitivity to data quality. Subsequent validation on carefully examined datasets will ascertain that these patterns are not mere data artifacts.

Conflict of interest

The author declares no competing financial interest.

Appendix

Table A1. Use of Parrot optimizer, GA and PSO

Component	Status	Purpose
Parrot Optimizer	Fully implemented	Membership function and weight tuning
Genetic Algorithm	Implemented as baseline	Performance comparison
PSO	Implemented as baseline	Performance comparison
Hybridization	Not used	Avoids methodological complexity

References

[1] E. Biermann, E. Cloete, and L. M. Venter, "A comparison of intrusion detection systems," *Computers & Security*, vol. 20, no. 8, pp. 676-683, 2001. https://doi.org/10.1016/s0167-4048(01)00806-9.

[2] T. Verwoerd and R. Hunt, "Intrusion detection techniques and approaches," *Computer Communications*, vol. 25, no. 15, pp. 1356-1365, 2002. https://doi.org/10.1016/S0140-3664(02)00037-3.

[3] A. Meryem and B. EL Ouahidi, "Importance of intrusion detection system (IDS)," *International Journal of Scientific & Engineering Research*, vol. 5, pp. 8-19, 2020. https://doi.org/10.1016/S1353-4858(20)30056-8.

[4] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Information Security Technical Report*, vol. 10, no. 3, pp. 134-139, 2005. https://doi.org/10.1016/j.istr.2005.08.001.

[5] J. Jabez and B. Muthukumar, "Intrusion detection system (IDS): Anomaly detection using outlier detection approach," *Procedia Computer Science*, vol. 48, pp. 338-346, 2015. https://doi.org/10.1016/j.procs.2015.04.191.

[6] A. I. Saleh, F. M. Talaat, and L. M. Labib, "A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers," *Artificial Intelligence Review*, vol. 51, no. 3, pp. 403-443, 2019. https://doi.org/10.1007/s10462-017-9567-1.

[7] S. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," In Proc. 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), Beijing, China, Jun. 4-6, 2016. pp. 581-585. https://doi.org/10.1109/iccsn.2016.7586590.

[8] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: Models, performance, challenges," *Artificial Intelligence Review*, vol. 55, no. 1, pp. 453-563, 2022. https://doi.org/10.1007/s10462-021-10037-9.

[9] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network intrusion detection system (IDS)," *International Journal of Information Security*, vol. 22, no. 5, pp. 1125-1162, 2023. https://doi.org/10.1007/s10207-023-00682-2.

[10] M. Alali, A. Almogren, M. M. Hassan, I. A. Rassan, and M. Z. A. Bhuiyan, "Improving risk assessment using fuzzy inference," *Computers & Security*, vol. 74, pp. 323-339, 2018. https://doi.org/10.1016/j.cose.2017.09.011.

[11] S. A. Abdymanapov, M. Muratbekov, S. Altynbek, and A. Barlybayev, "Fuzzy expert system for information security," *IEEE Access*, vol. 9, pp. 156556-156565, 2021. https://doi.org/10.1109/access.2021.3129488.

[12] A. P. H. de Gusmão, M. M. Silva, T. Poleto, L. C. e Silva, and A. P. C. S. Costa, "Cybersecurity risk analysis using fuzzy decision theory," *International Journal of Information Management*, vol. 43, pp. 248-260, 2018. https://doi.org/10.1016/j.ijinfomgt.2018.08.008.

[13] A. Namdari and Z. Li, "Review of entropy measures for uncertainty," *Advances in Mechanical Engineering*, vol. 11, no. 6, pp. 1-16, 2019. https://doi.org/10.1177/1687814019857350.

[14] K. J. DeMars, R. H. Bishop, and M. K. Jah, "Entropy-based uncertainty propagation," *Journal of Guidance, Control, and Dynamics*, vol. 36, no. 4, pp. 1047-1057, 2013. https://doi.org/10.2514/1.58987.

[15] Q. Zhang, C. Zhou, Y.-C, Tian, N. Xiong, Y. Qin, and B. Hu, "Fuzzy probability Bayesian network for cybersecurity risk assessment in industrial control systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2497-2506, 2017. https://doi.org/10.1109/tii.2017.2768998.

[16] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework for IoT," *Computers in Industry*, vol. 144, p. 103801, 2023. https://doi.org/10.1016/j.compind.2022.103801.

[17] I. H. Sarker, "Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," *Security and Privacy*, vol. 6, no. 5, p. e295, 2023. https://doi.org/10.1002/spy2.295.

[18] C. Soize, "Uncertainty quantification in computational structural dynamics and vibroacoustics," in *Uncertainty Quantification: An Accelerated Course with Advanced Applications in Computational Engineering*, Cham, Switzerland: Springer International Publishing, 2017, pp. 155-216. https://doi.org/10.1007/978-3-319-54339-0_8.

[19] J. Dai, W. Wang, Q. Xu, and H. Tian, "Uncertainty measurement using extended conditional entropy," *Knowledge-Based Systems*, vol. 27, pp. 443-450, 2012. https://doi.org/10.1016/j.knosys.2011.10.013.

[20] A. Thelen, X. Zhang, O. Fink, Y. Lu, S. Ghosh, B. D. Youn, et al., "A comprehensive review of digital twin–Part 2: Roles of uncertainty quantification and optimization, a battery digital twin, and perspectives," *Structural and Multidisciplinary Optimization*, vol. 66, no. 1, p. 1, 2023. https://doi.org/10.1007/s00158-022-03410-x.

[21] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based intrusion detection: Techniques and challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18-28, 2009. https://doi.org/10.1016/j.cose.2008.08.003.

[22] G. Kocher and G. Kumar, "ML/DL methods for IDS," *Soft Computing*, vol. 25, no. 15, pp. 9731-9763, 2021. https://doi.org/10.1007/s00500-021-05893-0.

[23] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion detection by machine learning," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994-12000, 2009. https://doi.org/10.1016/j.eswa.2009.05.029.

[24] S. Raponi, M. Caprolu, and R. Di Pietro, "Intrusion detection at the network edge: Solutions, limitations, and future directions," in *International Conference, Held as Part of the Services Conference Federation*, Cham: Springer, 2019, pp. 59-75. https://doi.org/10.1007/978-3-030-23374-7_5.

[25] A. Heidari and M. A. J. Jamali, "Internet of Things intrusion detection systems: A comprehensive review and future directions," *Cluster Computing*, vol. 26, no. 6, pp. 3753-3780, 2023. https://doi.org/10.1007/s10586-022-03776-z.

[26] R. Mitchell and I. R. Chen, "IDS for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1-29, 2014. https://doi.org/10.1145/2542049.

[27] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1-22, 2019. https://doi.org/10.1186/s42400-019-0038-7.

[28] R. Singh, H. Kumar, R. K. Singla, and R. R. Ketti, "Internet attacks and IDS," *Online Information Review*, vol. 41, no. 2, pp. 171-184, 2017. https://doi.org/10.1186/s42400-019-0038-7.

[29] C. Chatfield, "Model uncertainty, data mining, and statistical inference," *Journal of the Royal Statistical Society: Series A*, vol. 158, no. 3, pp. 419-466, 1995. https://doi.org/10.2307/2983440.

[30] D. Draper, "Assessment and propagation of model uncertainty," *Journal of the Royal Statistical Society: Series B*, vol. 57, no. 1, pp. 45-97, 1995. https://doi.org/10.1111/j.2517-6161.1995.tb02015.x.

[31] B. Möller and M. Beer, *Engineering Computation Under Uncertainty*. Berlin, Germany: Springer, 2008. https://doi.org/10.1016/j.compstruc.2007.05.041.

[32] J. L. Beck and L. S. Katafygiotis, "Updating Models and Their Uncertainties. I: Bayesian Statistical Framework," *Journal of Engineering Mechanics*, vol. 124, no. 4, pp. 455-461, 1998. https://doi.org/10.1061/(ASCE)0733-9399(1998)124:4(455).

[33] V. Rodriguez-Galiano, M. Sanchez-Castillo, M. Chica-Olmo, and M. Chica-Rivas, "Machine learning predictive models for mineral prospectivity: An evaluation of neural networks, random forest, regression trees and support vector machines," *Ore Geology Reviews*, vol. 71, pp. 804-818, 2015. https://doi.org/10.1016/j.oregeorev.2015.01.001.

[34] V. M. Lourenço, J. O. Ogutu, R. A. Rodrigues, A. Posekany, and H. P. Piepho, "Genomic prediction using machine learning: A comparison of the performance of regularized regression, ensemble, instance-based and deep learning methods on synthetic and empirical data," *BMC Genomics*, vol. 25, no. 1, p. 152, 2024. https://doi.org/10.1186/s12864-023-09933-x.

[35] A. Dinh, S. Miertschin, A. Young, and S. D. Mohanty, "A data-driven approach to predicting diabetes and cardiovascular disease with machine learning," *BMC Medical Informatics and Decision Making*, vol. 19, no. 1, p. 211, 2019. https://doi.org/10.1186/s12911-019-0918-5.

[36] L. Alzubaidi, J. Zhang, A. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, et al., "Review of deep learning," *Journal of Big Data*, vol. 8, pp. 1-60, 2021. https://doi.org/10.1186/s40537-021-00444-8.

[37] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A survey of deep learning and its applications: A new paradigm to machine learning," *Archives of Computational Methods in Engineering*, vol. 27, pp. 1071-1092, 2020. https://doi.org/10.1007/s11831-019-09344-w.

[38] M. Javeed, N. A. Mudawi, A. Alazeb, S. Almakdi, S.S. Alotaibi, S.A. Chelloug, et al., "Intelligent ADL recognition via IoT-based multimodal deep learning framework," *Sensors*, vol. 23, no. 18, p. 7927, 2023. https://doi.org/10.3390/s23187927.

[39] K. Kowsari, D. E. Brown, M. Heidarysafa, K. Jafari Meimandi, M. S. Gerber, and L. E. Barnes, "HDLTex: Hierarchical deep learning for text classification," In Proc. 2017 IEEE International Conference on Machine Learning and Applications, Cancun, Mexico, Dec. 18-21, 2017, pp. 364-371. https://doi.org/10.1109/ICMLA.2017.0-134.

[40] V. Singh, V. Kumar, and V. B. Singh, "A hybrid novel fuzzy AHP-TOPSIS technique for selecting parameter-influencing testing in software development," *Decision Analytics Journal*, vol. 6, p. 100159, 2023. https://doi.org/10.1016/j.dajour.2022.100159.

[41] M. Akram, Shumaiza, and J. C. Rodríguez Alcantud, "Enhanced decision making method with two-tuple linguistic bipolar fuzzy sets," in *Multi-criteria Decision Making Methods with Bipolar Fuzzy Sets*. Singapore: Springer, 2023, pp. 177-212. https://doi.org/10.1007/978-981-99-0569-0_7.

[42] S. J. H. Dehshiri and M. Amiri, "Evaluation of blockchain implementation solutions in the sustainable supply chain: A novel hybrid decision approach based on Z-numbers," *Expert Systems with Applications*, vol. 235, p. 121123, 2024. https://doi.org/10.1016/j.eswa.2023.121123.

[43] A. Mardani, A. Jusoh, and E. K. Zavadska, "Fuzzy multiple criteria decision-making techniques and applications–Two decades review from 1994 to 2014," *Expert Systems with Applications*, vol. 42, no. 8, pp. 4126-4148, 2015. https://doi.org/10.1016/j.eswa.2015.01.003.

[44] M. Saad, "NSL-KDD Dataset (KDDTrain+)," 2017. [online]. Available: https://raw.githubusercontent.com/Jehuty4949/NSL_KDD/master/KDDTrain+.csv. [Accessed Mar. 10, 2026].

[45] M. Saad, "NSL-KDD Dataset (KDDTest+)," 2017. [online]. Available: https://raw.githubusercontent.com/Jehuty4949/NSL_KDD/master/KDDTest+.csv. [Accessed Mar. 10, 2026].

[46] K. A. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of network attacks using machine learning and deep learning models," *Procedia Computer Science*, vol. 218, pp. 57-66, 2023. https://doi.org/10.1016/j.procs.2022.12.401.

[47] V. Kandasamy and A. A. Roseline, "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks," *Scientific Reports*, vol. 15, no. 1, p. 1697, 2025. https://doi.org/10.1038/s41598-025-85547-5.

[48] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395-9409, 2022. https://doi.org/10.1016/j.aej.2022.02.063.

[49] H. Rezaei, R. Taheri, M. Shojafar, and C. H. Foh, "GRAF-IDS: Graph-based clustering as aggregation for federated intrusion detection system in IoT network," *Neural Computing and Applications*, vol. 37, no. 22, pp. 18401-18423, 2025. https://doi.org/10.1007/s00521-025-11385-1.

[50] A. Meryem and B. E. Ouahidi, "Hybrid intrusion detection system using machine learning," *Network Security*, vol. 2020, no. 5, pp. 8-19, 2020. https://doi.org/10.1016/S1353-4858(20)30056-8.

[51] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1353-1374, 2022. https://doi.org/10.1007/s13369-021-05947-3.

[52] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: Machine learning for enhanced security," *Scientific Reports*, vol. 14, no. 1, p. 5872, 2024. https://doi.org/10.1038/s41598-024-56126-x.

[53] R. Vadisetty and A. Polamarasetti, "Enhancing intrusion detection systems with deep learning and machine learning algorithms for real-time threat classification," In Proc. 2024 Asian Conference on Intelligent Technologies, Pune, India, Sep. 6-7, 2024, pp. 1-6. https://doi.org/10.1109/ACOIT62457.2024.10939322.

[54] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

[55] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," In Proc. 2001 IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 14-16, 2001, pp. 130-143. https://dl.acm.org/doi/10.5555/882495.884435.

[56] H. Rezaei, R. Taheri, I. Jordanov, and S. Shiaeles, "Adapt-LFA: Adaptive gradient-guided label flipping attack against federated learning-based intrusion detection in IoT," In Proc. 2025 IEEE International Conference on Cyber Security and Resilience, Chania, Crete, Greece, Aug. 4-6, 2025, pp. 407-412. https://doi.org/10.1109/CSR64739.2025.11130071.

[57] H. Rezaei, R. Taheri, I. Jordanov, and M. Shojafar, "Federated RNN for intrusion detection system in IoT environment under adversarial attack," *Journal of Network and Systems Management*, vol. 33, no. 4, p. 82, 2025. https://doi.org/10.1007/s10922-025-09963-8.

[58] L. Liu, G. Engelen, T. Lynar, D. Essam, and W. Joosen, "Error prevalence in NIDS datasets: A case study on CIC-IDS-2017 and CSE-CIC-IDS-2018," In Proc. 2022 IEEE Conference on Communications and Network Security, Austin, TX, USA, Oct. 24-26, 2022, pp. 254-262. https://doi.org/10.1109/CNS56114.2022.9947235.