NSS
Neutrosophic Sets and Systems, Vol. 97, 2026
University of New Mexico

A new Neutrosophic Paradox Distribution with Application in Modeling Cyber-Attack Uncertainty

Nahed I. Isa[1,*], Hegazy M. Zaher[2], Noura A. T. Abu El-Magd[3]

[1]Faculty of Graduate Studies for Statistical Research, Cairo University, Giza, Egypt.

[2] Faculty of Graduate Studies for Statistical Research, Cairo University, Giza, Egypt.

[3] Faculty of Politics and Economics, Beni-Suef University, Beni-Suef, Egypt.

*Corresponding Author: nahed.eassa@yahoo.com

Abstract In recent years, researchers have increasingly focused on neutrosophic probability distributions to handle incomplete data and inherent uncertainty. A novel distribution, called the Neutrosophic Paradox Distribution (NPD), will be introduced in this paper, which is developed using neutrosophic algebra in a unique and innovative manner. The NPD is constructed from three underlying component distributions, and we thoroughly investigate its mathematical characteristics, such as mean, variance, and cumulative function, including a formal proof of its neutrosophic probability density function. To illustrate its practical utility, we present detailed examples of specific NPD components such as the Beta-Neutrosophic Paradox Distribution (Beta-NPD) and the Exponential-Neutrosophic Paradox Distribution (Exponential-NPD). Furthermore, the proposed distribution is applied to devise robust solutions for complex cybersecurity problems. In this paper, solved examples are presented to clarify the effectiveness and applicable to apply of NPD in real-world scenarios, highlighting its potential as a valuable tool in uncertain and incomplete data environments.

Keywords: neutrosophic paradox distribution; Beta distribution; Exponential distribution; machine learning; cybersecurity.

1. Introduction

Florentine Smarandache introduced Neutrosophic logic in (1999), which is essential when dealing with incomplete, inconsistent, or generalizes classical, fuzzy, and intuitionistic fuzzy logics by introducing three independent components: these degrees called truth (T), indeterminacy (I), falsity (F) unlike traditional frameworks that consider only degrees of truth or membership, neutrosophic logic models uncertainty more comprehensively by explicitly incorporating indeterminacy contradictory information [1-4].

This triadic approach has inspired the development of several neutrosophic statistical distributions, including the neutrosophic Weibull [5,6], neutrosophic exponential [7,8], neutrosophic normal distribution [9,10], neutrosophic multinomial distribution, neutrosophic binomial distribution [11], neutrosophic Poisson [12], neutrosophic beta distribution [13] and neutrosophic Gamma distributions, which aim to model uncertainty and contradictions in various domains [14,15]. Neutrosophic Rayleigh [16]. These distributions extend classical distributions by incorporating indeterminacy (I) into the framework, allowing for more flexible and accurate modeling of real-world phenomena.

For example, the Neutrosophic Generalized Pareto Distribution (NGPD) has been effectively applied to financial modeling, particularly in capturing extreme events and fluctuations in public debt under uncertain conditions.[17,18]. The neutrosophic models have been applied in cybersecurity [19, 20]. However, classical probabilistic models remain inadequate for handling paradoxical evidence, where data simultaneously support conflicting hypotheses, such as normal and abnormal network behavior in cybersecurity. To address this, the Neutrosophic Paradox Distribution (NPD) has been introduced as a novel statistical framework that explicitly represents contradictions and indeterminacy, making it particularly suitable for complex threat environments. Unlike traditional models, NPD treats contradictions as inherent system features rather than errors, providing a robust tool for anomaly detection and threat analysis where data is often incomplete, noisy, or conflicting. This

is especially relevant in scenarios like distributed denial-of-service (DDoS) attack detection, where traffic patterns may exhibit both benign and malicious characteristics, challenging binary classification approaches.

While a unified formalism for neutrosophic distributions is still evolving, some researchers advocate representing parameters, variables, or probability density functions as triplets (T, I, F) to capture ambiguity directly within the statistical model [9]. This approach aligns with the broader neutrosophic philosophy of embracing uncertainty and indeterminacy, thus offering a powerful extension to classical and fuzzy statistical methods for diverse applications in cybersecurity, finance, and beyond.

Furthermore, this paper is organized as follows: In Section 2, we present definitions and the formulation of the NPD. A derives key statistical functions, including Probability Density Function (PDF), Cumulative Distribution Function (CDF), and the hazard rate, presented in section 3. Section 4 offers practical examples demonstrating the application of NPD to real-world data. Lastly, we summarize the main findings and outline potential areas for future work in Section 5.

2. Neutrosophic Paradox Distribution (NPD)

Inspired by Smarandash's theory of neutrosophic probability [21] and the need to model paradoxical uncertainty, we propose a new distribution called the neutrosophic paradox distribution (NPD), which is designed to represent uncertain, ambiguous, paradoxical data by modeling three levels (true, uncertainty, and false) in a probability distribution. Let X be a random variable with the following properties:
T(x): the degree of truth for x
I(x): the degree of indeterminacy for x.
F(x) is the degree of falsehood for x.
PDF for the NPD can be represented as a function of these three components, taking into account that the sum of these components can exceed one.

$$f_{NP}(X) = \mathrm{T}(x) + I(x) + F(X)$$

Where:

- $0 \leq \mathrm{T}, \mathrm{I}, \mathrm{F} \leq 1$ and $0 \leq \mathrm{T} + \mathrm{I} + \mathrm{F} \leq 3$

  (Smarandache (2015)

- T(x) is probability where x represents true outcome.
- I(x) is a probability where x represents an indeterminate outcome.
- F(x) is the probability where x represents a false outcome.

3. The NPD properties

In this section, properties of NPD, statistical properties such as variance, mean, and special cases, will be introduced.

3.1 Non-Normalized Distribution

The Neutrosophic Paradox Distribution is not necessarily normalized to sum to 1. This is because it includes three parts: truth, uncertainty, and Falsehood; each part has its value or distribution. As a result, their sum may not exactly equal one. If necessary, we can normalize the values by conforming them so that their sum equals one. This is done by conforming to the weight of each part.

$$f(x)_{normalized} = \frac{f_T(x) + f_I(x) + f_F(x)}{\sum f_T(x) + f_I(x) + f_F(x)}$$

3.2 Flexibility in Component Distributions

The Neutrosophic Paradox Distribution (NPD) allows for flexibility in the choice of distributions for the three components (Truth, Indeterminacy, and Falsehood). Each component may be modeled using different distributions, according to the

nature data and applications at hand. This allows the NPD to deal with a wide assortment of data types.

For example:

- The Truth component may follow a Beta or Normal distribution, depending on whether the data is bounded or unbounded.
- The Indeterminacy component might be modeled using Gamma or Uniform distributions to capture different types of uncertainty.
- The Falsehood component may follow distributions like Exponential or Weibull to model rare or decaying events.

3.3 Parameters of the Distribution

Each component $f_T(x), f_I(x,)\ and f_F(x)$ will have its own set of parameters, depending on the chosen distribution. These parameters control the shape and scale of the distributions:

- Truth (T): Parameters might include α_T and β_T for a Beta distribution, or mean and standard deviation for a Normal distribution.
- Indeterminacy (I): Parameters might include shape and scale for a Gamma distribution or a and b for a Uniform distribution.
- Falsehood (F): Parameters might include the rate for an Exponential distribution or the scale for a Weibull distribution.

3.4 Non-Symmetry

Unlike the Normal distribution, the Neutrosophic Paradox Distribution is non-symmetric by design. Since it combines multiple components representing truth, uncertainty, and falsehood, the performing distribution may exhibit skewness or asymmetry. This feature allows the distribution to model more complex real-world phenomena where data does not follow a symmetrical pattern

3.5 Skewness and Kurtosis

The Neutrosophic Paradox Distribution can exhibit skewness (the asymmetry of the distribution) and kurtosis depending on the choice of distributions for each component:

- If the Truth component is modeled using a Beta distribution, the resulting distribution can be swerved according to specific values of its parameters.α_T and β_T.
- Indeterminacy components may also introduce skewness or heavy tails if they follow a Gamma or Exponential distribution.
- The Falsehood component, especially when modeled with an Exponential or Weibull distribution, can yield a distribution with heavy tails.

3.6 Cumulative Distribution Function (CDF)

$$F_{NPD}(x) = F_T(x) + F_I(x) + F_F(x)$$

Where:

- $F_T(x)$ is the CDF of the Truth component.
- $F_I(x)$ is the CDF of the Indeterminacy component.
- $F_F(x)$ is the CDF of the Falsehood component.

3.7 Mean and Variance

i. The expected value (μ) and the variance (σ) of the NPD can be deduced by calculating the mean and variance of each of its components. Since the distribution is the sum of these components, the overall mean and variance are the sums of the means and variances of the individual components.

The mean of the NPD can be computed as:

$$\mu_{NPD} = \mu_T + \mu_I + \mu_F$$

Where μ_T, μ_I, and μ_F are the means of the Truth, Indeterminacy, and Falsehood components, respectively.

ii. The variance of the NPD can be computed as:

$$\sigma^2_{NPD} = \sigma^2_T + \sigma^2_I + \sigma^2_F$$

Where σ^2_T, σ^2_I and σ^2_F are the variances of the Truth, Indeterminacy, and Falsehood components, respectively.

3.8 Additive Nature of Components

One of the main properties of the Neutrosophic Paradox Distribution (NPD) is its additive nature. The overall distribution is a sum of three distinct components, each of which contributes to the overall behavior of the system. This allows for flexible modeling of complex phenomena, where different levels of truth, uncertainty, and falsehood may be attended.

3.8 Handling Paradoxical Data

The Neutrosophic Paradox Distribution is particularly useful for paradoxical data where the standard assumptions of classical distributions (such as normality) do not apply. This makes it a powerful tool for modeling real-world problems in areas like cybersecurity, finance, and decision-making, where data often contains conflicting or contradictory information.

3.10 The Application of NPD

The Neutrosophic Paradox Distribution (NPD) is a versatile modeling of uncertainty, indeterminacy, and falsehood in various systems. Its key properties, such as flexibility in component distributions, non-normalization, and the additive nature of its components, make it suitable for handling complex and paradoxical data. Understanding these properties is crucial for applying the NPD in real-world applications and making informed decisions based on uncertain or conflicting information.

Applications:

- Modeling systems with inherent contradictions.
- Decision-making under paradoxical uncertainty.
- Complex systems where classical probability fails.

4. Examples for Components of NPD and its Mathematical Properties

4.1 Beta-NPD

The Neutrosophic Paradox Distribution (NPD) is defined in terms of a tripartite distribution function for a random variable x, where T(x), I(x) and F(x) follow specific parametric forms. The total distribution is then a combination of these components.

Probability Distribution Components:

Let us assume each component follows a Beta distribution, which is commonly used to model uncertainty:

$$T(x) \sim Beta(\alpha_T, \beta_T)$$
$$I(x) \sim Beta(\alpha_I, \beta_I)$$
$$F(x) \sim Beta(\alpha_F, \beta_F)$$

Where $\alpha_T, \alpha_I, \alpha_F$, and $\beta_T,\ \beta_I, \beta_F$ are shape parameters that govern the distribution of truth, indeterminacy, and falsehood, respectively. These parameters can be adjusted to simulate different levels of indeterminacy in the data.

- **General Mathematical formulation of Beta-NPD:**

The general form of the Neutrosophic Paradox Distribution (NPD) can be written as:

$$f_{NP}(X) = \left(\frac{x^{\alpha_T-1}(1-x)^{\beta_T-1}}{B(\alpha_T,\beta_T)}\right) + \left(\frac{x^{\alpha_I-1}(1-x)^{\beta_I-1}}{B(\alpha_I,\beta_I)}\right) + \left(\frac{x^{\alpha_F-1}(1-x)^{\beta_F-1}}{B(\alpha_F,\beta_F)}\right),$$
$$0 \le x \le 1$$

Where:

- B (α, β) is the Beta function, which normalizes the Beta distribution so that the total area under the curve is 1.
- The components T(x), I(x), and F(x) are integrated to provide a total distribution f(x) that accounts for truth, indeterminacy, and falsehood.

▪ Parameterization of Beta-NPD

- α_T, β_T control the distribution of the truth component.
- α_I, β_I control the distribution of the indeterminacy component.
- α_F, β_F control the distribution of the falsehood component.

Interpretation of the Parameters

- A high value of α_T and a low value of β_T indicate a high confidence in the truth component of the data.
- A high value ofα_I and a low value of β_I represent higher indeterminacy (i.e., greater uncertainty).
- A high value of α_F and a low value of β_F suggest a strong presence of falsehood in the data.

By adjusting these parameters, you can simulate different levels of paradoxical behavior, where the data simultaneously contains truth, indeterminacy, and falsehood.

Important Notes

1. The sum f(x) is not a probability distribution in the classical sense, because it can exceed 1 (since T + I + F can be > 1 in neutrosophy).
2. Each component (T, I, F) is a valid Beta distribution (i.e., its area = 1).
3. We use separate parameters (α,β) for each component to model their behaviors independently.

▪ Simulation

To simulate and visualize the Neutrosophic Paradox Distribution (NPD) in this case, I implemented the distribution in Python using the scipy.stats.beta module to generate the three-neutrosophic components: Truth (T), Indeterminacy (I), and Falsehood (F). Each component was modeled using a different Beta distribution: T(x) ~ Beta (2.5, 5.0), I(x) ~ Beta (3.0, 3.0), and F(x) ~ Beta (5.0, 2.0). These choices were made to reflect different probabilistic behaviors over the normalized feature space [0, 1]. The final NPD(x) was computed as the sum of the three components, illustrating the paradoxical overlap and interplay between them. The simulation was conducted in Python and visualized using matplotlib, allowing an intuitive comparison between the individual components and their combined effect in the NPD frame.

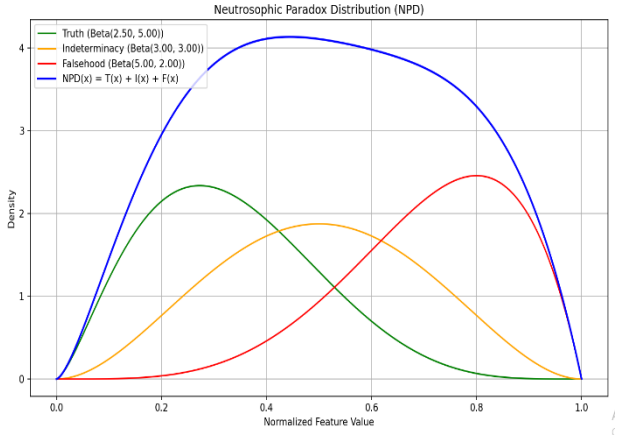

Figure 1: The simulation plot of the NPD using cybersecurity data.

Figure 1: shows the Neutrosophic Paradox Distribution (NPD) using simulated cybersecurity data, where:

- The green curve: presents the beta distribution for truth (t), which is ' benign traffic'.
- The Orange curve: indeterminacy (I), which captures the uncertainty region, where it is not clear whether behavior is benign or This component is crucial because it gives paradoxical behavior, where the system is unsure, helpful for zero-day attacks or new, unseen patterns. Malicious.
- The Red curve: falsehood (F) Models malicious or anomalous behavior, such as DDoS or PortScan attacks.

The Blue curve: This is the final Neutrosophic Paradox Distribution. It combines all three components: truth, falsehood, and indeterminacy, and gives a holistic view of data behavior across the entire domain (e.g., normalized feature values between 0 and 1).

This is important because:

- Traditional models treat either data as "normal" or "anomalous".
- The NPD plot shows three views at once, accepting the paradox that uncertainty exists.
- It helps in better thresholding and confidence scoring for classification:
  - High T(x) → likely normal
  - High F(x) → likely attack
  - High I(x) → suspicious or ambiguous, may require deeper analysis

While we previously assumed that each component follows a Beta distribution, it is important to highlight that different distributions can be chosen for each component. For example:

- Truth (T): You might use a Beta, Gaussian, or Lognormal distribution, depending on whether you believe the data's truthfulness follows a bounded or unbounded pattern.

Indeterminacy (I): The Gamma, Normal, or Uniform distributions might be appropriate if the indeterminacy is uniformly distributed or follows a skewed distribution. table 1 shows how we can choose the function model indeterminacy

Table 1: The function indeterminacy I (t)

Function	Behaviour	Recommended Applications

Exponential decay γte^{-t}	Indeterminacy decreases over time and distance	Systems with memory (e.g., mechanical wear)
Lorentizian $\frac{\gamma}{1+t^2}$	Slow decay with long tails	Social systems, slow-changing environments
Gamma $\gamma t^{k-1}e^{-t/\delta}$	Peaks then decay	Temporary phenomena (e.g., disease outbreaks)
$\gamma sin^2(\omega x)$ γ: Amplitude (scales max indeterminacy to $[0, \gamma]$). ω: frequency (controls oscillation speed; $\omega = \frac{2\pi}{t}\ for\ period\ T$	Peaks at γ (max indeterminacy) when $\gamma sin^2(\omega x) = 1$ Drops to 0 (no indeterminacy) at $\gamma sin^2(\omega x) = 0$	Periodic Attacks Models attacks recurring at fixed intervals (e.g., scheduled scans/campaigns).

- Normalization: ensure max(I(t) ≤ 1) via:

$$I(t) = \gamma.\frac{raw\ intensity}{\max observed\ intensity}$$

- Falsehood (F): For falsehood, you could choose distributions such as Exponential, Weibull, or Beta to capture various forms of decay or uncertainty.

Thus, the components T(x), I(x), and F(x) can follow any appropriate distribution, providing flexibility for modelling the paradoxical behaviour of data.

4.2 The Neutrosophic Exponential Paradox Distribution

We now define the Neutrosophic Exponential Paradox Distribution, introducing parameters α and β to handle indeterminacy and paradox levels.

Let λ>0, α, β∈ [0, 1], then:

Probability Density Function (PDF)

$$f_{NPD}(x;\lambda,\alpha,\beta) = (1-\alpha-\beta)\lambda e^{-\lambda x} + \alpha.\delta(x) + \beta.\lambda^2 x e^{-\lambda x}\ \ , x \geq 0$$

Where:

- $(1-\alpha-\beta)\lambda e^{-\lambda x}$Classical exponential (truth).
- $\alpha.\delta(x)$: Dirac delta function representing indeterminacy at point (uncertain/noisy)
- $\beta.\lambda^2 x e^{-\lambda x}$: Paradoxical behavior modelled via gamma (2, λ).

This distribution allows us to recover the exponential distribution when α = β = 0 and introduce uncertainty (α) and paradoxical influence (β).
The Properties of the Neutrosophic Exponential Paradox Distribution:

1. The Cumulative Distribution Function (CDF)

LET: $F_E(x) = 1 - e^{-\lambda x}$

And

$F_p(x) = 1 - e^{-\lambda x}(1 + \lambda x)$

Then the CDF OF NPD is:

$$F_{NPD}(x) = (1 - \alpha - \beta)\, F_E(x) + \beta F_p(x)$$

(The delta component does not contribute to the CDF science; it is a point mass.)

- To ensure the PDF integrates with 1:
- $(1 - \alpha - \beta) + \alpha + \beta = 1 \Rightarrow \alpha + \beta \leq 1$

α: degree of indeterminacy (noise, incomplete info).

β: degree of paradox (contradictory behavior).

λ: scale parameter (same as exponential).

2. The Mean of the NPD:

$\mu_{NPD} = \omega_T . E[X_E] + \omega_I E[X_I] + \omega_P E[X_P]$

- Given weights:

Truth component: $\omega_T = 1 - \alpha - \beta$

Indeterminate component: $\omega_I = \alpha$

Paradox component: $\omega_P = \beta$

$$E[X_E] = \frac{1}{\lambda}(mean\ of\ exponential)$$

$$E[X_I] = 0\ direct\ delta\ as\ zero$$

$$E[X_P] = \frac{2}{\lambda}\ (mean\ of\ Gamma\ (2, \lambda)$$

So:

$$\mu_{NPD} = (1 - \alpha - \beta)\frac{1}{\lambda} + 0 + \beta\frac{2}{\lambda}$$

$$\mu_{NPD} = \frac{(1 - \alpha + \beta)}{\lambda}$$

The Variance of the NLD:

$$var_{NPD} = \omega_T . Var[X_E] + \omega_P Var[X_P] + \omega_T(\mu_E - \mu_{NPD})^2 + \omega_P(\mu_P - \mu_{NPD})^2$$

This implementation shows how classical probability distributions can be extended to handle more complex, real-world situations where truth is not absolute but exists in degrees with inherent uncertainty.

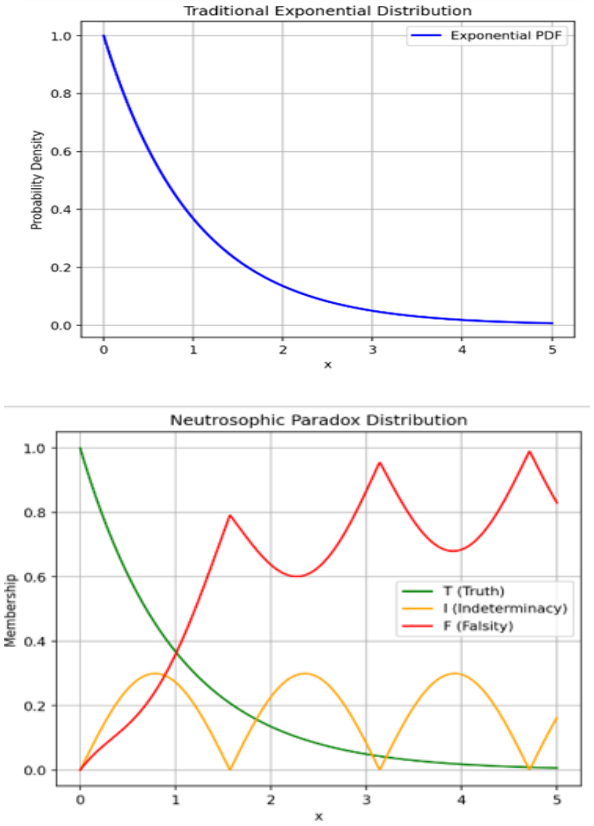

Figure 2: The difference between the traditional exponential distribution

and NPD

Figure 2 shows the difference between the traditional exponential distribution and the Neutrosophic Paradox Distribution as shown below:

- The traditional exponential is a pure probability distribution (values represent likelihoods)
- The neutrosophic version is more about membership degrees (truth, uncertainty, falsity)
- The neutrosophic approach can model systems where events have inherent uncertainty or a contradictory nature.

5 Real-world Cybersecurity Applications of the Neutrosophic Paradox Distribution (NPD)

This application presents an innovative machine-learning framework for detecting distributed denial of service (DDoS) attacks, which incorporates neutrosophic logic to handle uncertainty in network traffic classification. By transforming traditional network features into three-valued neutrosophic components (Truth, Indeterminacy, and Falsehood), the model effectively captures the ambiguous nature of modern cyber threats. The system automatically optimizes decision thresholds and combines classical statistical features with neutrosophic logic.

5.1 Methodology Steps:

5.1.1 Data source:

"CIC-IDS2017""Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv" containing labelled DDoS and benign network traffic flows. Feature Selection: The top 5 discriminative features were selected via ANOVA F-test ($p < 0.01$) to reduce dimensionality while preserving attack patterns Figure 3.

5.1.2 Data Preprocessing

i.Load and clean the dataset (handle missing values, infinity, label encoding).

- Convert labels (BENIGN=0, DDoS=1).

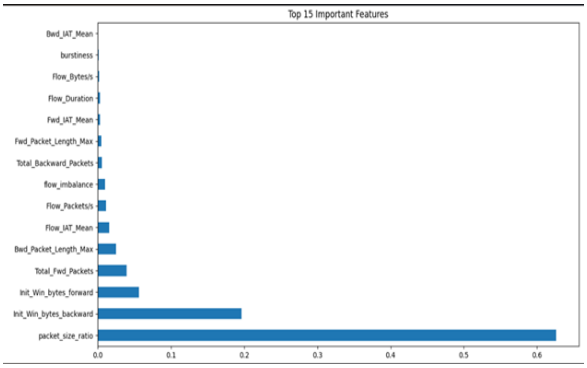

Figure 3: Top 15 important features.

5.1.3 Neutrosophic Transformation

- For each feature, dynamically calculate thresholds.
- Split feature values into Truth (T), Indeterminacy (I), and Falsehood (F) components as shown in Figure 4:
- T: Values > threshold (clear attack signatures).
- I: Values ∈ (0.5×threshold, threshold] (ambiguous traffic).
- F: Values ≤ 0.5×threshold (normal traffic).

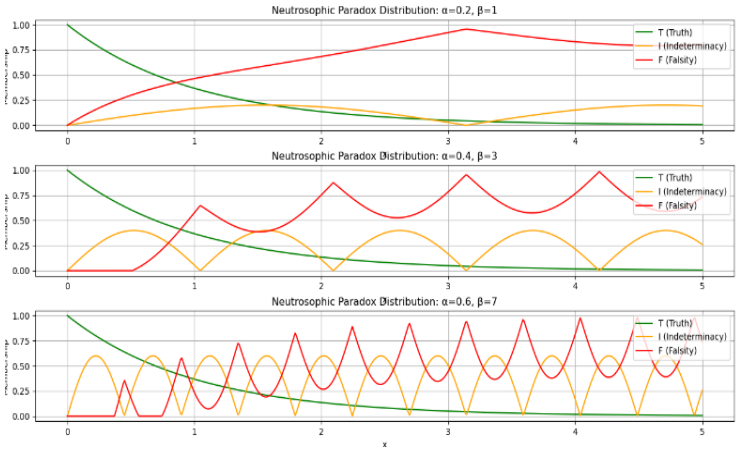

Figure 4: The threshold for some features using cybersecurity data

5.2 Threshold Optimization

Automatically select optimal thresholds using cross-validated F1-score.

5.3 Model Training

Train an XGBoost classifier using:

- 200 trees
- Depth of 7

- Learning rate = 0.05
- Balanced class weights

 Suitable for imbalanced data scenarios like attack detection

Sets the number of decision trees in the ensemble.200 trees provide sufficient diversity to improve detection accuracy while avoiding excessive computation.

5.4 empirically optimized

For DDoS detection, the following hyperparameter configuration was adopted:

- max_depth=7

This depth allows the model to handle intricate and nonlinear attack signatures commonly found in DDoS traffic, without excessively overfitting to noise or outliers.

- n_estimators = 200

Ensures a diverse and strong ensemble of decision trees for robust detection across various DDoS patterns.

6. Visualize the confusion matrix and neutrosophic distributions

6.1 Confusion Matrix

Representations, achieving enhanced detection capability, particularly for borderline cases. By integrating the degrees of truth, indeterminacy, and paradox, the model achieved more nuanced decision boundaries, reducing misclassification in ambiguous traffic flows as shown in Fig.5.

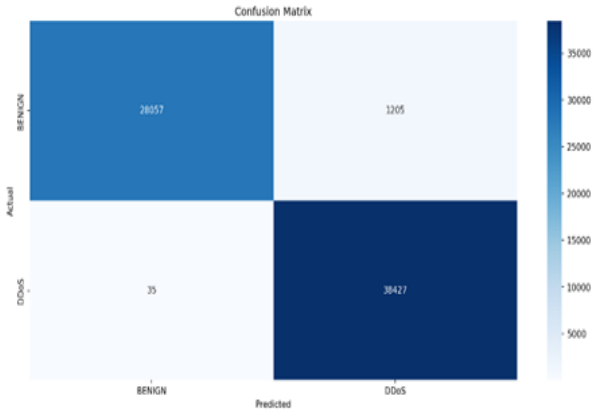

Figure 5: confusion matrix

6.2 Evaluation Metrics

Table 2. Classification Report: Precision, Recall, F1-score.

Table 2: Report precision/recall/F1-score achieved by the XGBoost classifier using neutrosophic representation for DDoS detection.

	precision	recall	f1-score	support
0	1.00	0.96	0.98	29262

1	0.97	1.00	0.98	38462
Accuracy			0.98	67724
Macro avg.	0.98	0.98	0.98	67724
Weighted avg.	0.98	0.98	0.98	67724

6.3 Performance Interpretation

It is clear from Table 2 that the proposed model exhibits a high accuracy of 98%, with a balanced precision-recall trade-off, achieving an F1-score of 0.98 for both benign and attack classes.

In particular, the classifier achieves perfect recall (1.00) for DDoS attacks, which means that all attack instances were correctly detected. At the same time, it maintains a high precision of 0.97, indicating a low rate of false positives of 0.1%. This reflects the robustness of the model in detecting DDoS attacks reliably and efficiently.

The 4% missed benign cases (that is, 96% recall for class 0) reflect a security-first design philosophy, prioritizing attack prevention over benign traffic throughput. This trade-off is acceptable in cybersecurity contexts where undetected attacks pose a greater risk than occasional benign misclassification.

7. Conclusion

In this paper, we demonstrate strong performance on unbalanced network datasets, suggesting that this hybrid approach could significantly improve real-world intrusion detection systems by providing interpretable decision boundaries for security analysts. This implementation relies on XGBoost with custom class balancing, which makes it computationally efficient in operational environments.

Integration of neutrosophic logic with machine learning investigate for future work using natural language processing models and deep learning methods for optical character recognition (OCR). By integrating the strength of neutrosophic logic in managing uncertainty and contradictory information with these powerful models, we aim to enhance performance in complex and noisy data environments. This hybrid approach has the potential to create more robust, interpretable, and efficient AI systems applicable to cybersecurity, text analysis, and image recognition tasks. Additionally, optimizing the interaction between neutrosophic representations and machine learning architectures, including automated threshold selection, will be an important focus for practical applications.

REFERENCES

[1] F. Smarandache and H. E. Khalid, Neutrosophic Precalculus and Neutrosophic Calculus, University of New Mexico, Infinite Study, 2018.

[2] F. Smarandache, “Neutrosophy and neutrosophic logic,” in Proceedings of the First International Conference on Neutrosophy, Neutrosophic Logic, Set, Probability, and Statistics, University of New Mexico, Gallup, NM 87301, USA, 1 December 2002.

[3] F. Smarandache, Introduction to Neutrosophic Measure, Integral, Probability, Sitech Education publisher, 2015.

[4] S. Kumar, M. Singh, A review on Neutrosophic Logic and its application in Decision Making and Pattern Recognition. International Journal of Computer Science and Information Security, VOL.15, NO.5, pp.189–196, 2017.

[5] M. Jdid, "Inverse transformation to generate neutrosophic random variables following Weibull and geometric distributions," *HyperSoft Set Methods in Engineering*, vol. 1, pp. 141–154, 2024.

[6] F. Smarandache, K. Hamza, K. Fawzi, H. Alhasan, Neutrosophic Weibull distribution and Neutrosophic Family Weibull Distribution. Neutrosophic Sets and *Systems*, VOL.*28*, NO.1,2019

[7] M. Aslam, Design of Sampling Plan for Exponential Distribution under Neutrosophic Statistical Interval Method, IEEE Access, vol

2018, NO.6, 64153–64158, 2018.

[8] W.-Q. Duan, Z. Khan, M. Gulistan, and A. Khurshid, Neutrosophic exponential distribution: modeling and applications for complex data analysis, Complexity, vol. 2021, Article ID 5970613, 8 pages, 2021.

[9] R. A. K. Sherwani, M. Aslam, M. A. Raza, M. Farooq, M. Abid, and M. Tahir, Neutrosophic normal probability distribution spine of parametric neutrosophic statistical tests: properties and applications," in Neutrosophic Operational Research, pp. 153–169, Springer, Berlin, Germany, 2021.

[10] S. K. Patro and F. Smarandache, Neutrosophic Statistics Distribution, more Problems, more solutions," Neutrosophic Sets and Systems, vol. 12, 2016.

[11] F. Smarandache, "Neutrosophic statistics is an extension of interval statistics, while plithogenic statistics is the most general form of statistics (second version)," *International Journal of Neutrosophic Science*, vol. 19, no. 1, pp. 148–165, 2022.

[12] R. Alhabib, M. M. Ranna, H. Farah, and A. A. Salama, Some neutrosophic probability distributions, Neutrosophic Sets and Systems, vol. 38, pp. 30–38, 2018.

[13] R. A. K. Sherwan, M. Naeem, M. Aslam, M. A. Raza, M. Abid, and S. Abbas, Neutrosophic beta distribution with properties and applications," Neutrosophic Sets Syst, vol. 41, pp. 209–214, 2021.

[14] A. M. Almarashi , M. Aslam, Process monitoring for gamma distributed product under neutrosophic statistics using resampling scheme, Jurnal Matematika, vol. 2021, Article ID 6635846, 12 pages, 2021.

[15] L. A. Zadeh, Fuzzy sets. Information and Control, VOL.8, NO.3, pp.338–353, 1965. https://doi.org/10.1016/S0019-9958(65)90241-X

[16] Z. Khan, M. Gulistian, N. Kausar,C.Park. Neutrosophic Rayleigh Model with Some Basic Characteristics and

Engineering Applications, IEEE Access, vol. 9, 7127-71283, 2021

[17] N. Eassa, H. Zaher, N. Abu El-Magd, "Neutrosophic Generalized Pareto Distribution," Mathematics and Statistics, Vol. 11, No. 5, pp. 827 - 833, DOI: 10.13189/ms.2023.110509. 2023.

[18] E. Plimi, A. Mundher, T. Mohammed, O. Adebowale, A. Oluwole, A New Generalization of the Lomax Distribution with Increasing, Decreasing, and Constant Failure Rate, Hindawi Modelling and Simulation in Engineering Volume 2017, ID 6043169, 6 pages 2017.

[19] M. A. Al-Hagery and A. I. A. Musa, "Enhancing network security using possibility neutrosophic hypersoft set for cyberattack detection," International Journal of Neutrosophic Science, vol. 25, no. 3, pp. 103-115, June 2024.

[20] H. S. Al-Khazraji, A. M. Alkhamees, H. M. Al-Doori, A. A. Metwaly, M. Eassa, A. Abdelhafeez, A. S. Salama, and A. M. Nagm, "Machine learning models with neutrosophic numbers for network anomaly detection and security defense technology," *Neutrosophic Sets and Systems*, vol. 83, pp. 1–14, 2025.

[21] S. Broumi, F. Smarandache, Neutrosophic Decision Making in Artificial Intelligence. Neutrosophic Sets and Systems, VOL. 2020, NO.1, 2020

.

Received: May 26, 2025. Accepted: Nov 9, 2025