Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 01 (2026)

Cyber Threat Evaluation Using Neutrosophic Hyper Soft Rough Matrices: A TOPSIS-Based MCDM Method

J. Boobalan[1] E.Mathivadhana[2,*]

[1,2] Department of Mathematics, Annamalai University, Annamalai Nagar, Chidambaram, India.
[1]jboobalan@hotmail.com, [2]mathivadhana99@gmail.com

[1]Department of Mathematics, Manbumigu Dr. Puratchithalaivar M.G.R. Government Arts and Science College, Keezha Vanniyur, Kumaratchi - 608 302, India.

Abstract:- Cybersecurity monitoring systems continuously generate heterogeneous and uncertain alerts, making reliable threat prioritization a complex challenge. Traditional decision-making models are limited in their ability to quantify indeterminacy arising from dynamic attack conditions and incomplete security evidence. To address this issue, this paper proposes a Technique for Order Preference by Similarity to Ideal Solution (TOPSIS)-based Multi-criteria decision making (MCDM) method built on the Neutrosophic Hyper Soft Rough Matrix (NHSRM) framework. A MATLAB code is given to demonstrate the computational procedure of the proposed method, involving neutrosophic matrix formation, normalization, weighted aggregation, and closeness coefficient computation. Experimental outcomes indicate that attacks exploiting service disruption and unauthorized internal access pose greater operational impact compared to well-mitigated malware-based threats, reflecting the current maturity of defensive technologies in that domain. Sensitivity analysis highlights that inappropriate weight selection can lead to suboptimal threat ranking; therefore, periodic weight adjustment based on evolving attack intelligence is recommended.

Keywords: *Cybersecurity, Neutrosophic Hyper Soft Rough Matrix, TOPSIS-MCDM, Threat prioritization, MATLAB code.*

1. Introduction

In the era of hyperconnected digital ecosystems, cybersecurity systems must process vast volumes of uncertain, conflicting, and time-varying data. Alerts from firewalls, intrusion detection systems (IDS), antivirus tools, user access logs, and network monitors often contain ambiguous and inconsistent information, leading to uncertainty in assessing real-time system security. The rapid evolution of cyber threats, coupled with heterogeneous data sources and fluctuating operational contexts, further complicates the task of deriving accurate and timely security decisions.

Conventional uncertainty-handling frameworks such as fuzzy sets, rough sets, and probabilistic theories attempt to mitigate these challenges but remain limited to single-dimensional or two-dimensional uncertainty representations. Moreover, these models do not accommodate the multi-attribute, multi-layer nature of modern cyber defence systems, where attributes such as severity, frequency, temporal pattern, device criticality, user privilege level, anomaly intensity, and contextual behaviour evolve dynamically and influence one another.

NHSRM overcome these limitations by providing an advanced mathematical environment capable of handling multi-attribute, multi-subattribute structures while explicitly modelling three-dimensional uncertainty. NHSRM allow decision-makers to represent complex cyber alerts in a hierarchical and granular form, where attributes may have nested components, each exhibiting its own degree of truth, indeterminacy, and falsity. This enables a much

more nuanced representation of cyber risk, reflecting both the uncertainty within individual alert sources and the uncertainty across interdependent cyber layers.

1.1 Literature Review

Cybersecurity has evolved into a complex decision-making domain characterized by ambiguity, incomplete information, and dynamically changing threat conditions. Classical mathematical tools have provided foundational approaches for modelling uncertainty. Fuzzy set theory, introduced by Zadeh [26], enabled the representation of approximate reasoning, while Atanassov's intuitionistic fuzzy sets [4] extended this framework by incorporating membership and non-membership degrees. Complementing these, soft set theory by Molodtsov [14] and rough set theory by Pawlak [16] established mechanisms for handling parameterization and boundary-based approximations in information systems.

Building on these foundations, recent works have enhanced multi-criteria decision-making (MCDM) under uncertainty. Sahoo et al. [17] compiled advanced methodologies for decision-making under uncertainty, encompassing optimization, modelling, and analytical frameworks. Their work highlights practical and theoretical approaches for handling imprecise, incomplete, or conflicting information in complex decision environments. Bhowmik et al. [5] developed a TOPSIS-based MAGDM approach using linguistic Z-numbers to capture both uncertainty and reliability in expert judgments. Their method improves decision-making accuracy in imprecise and confidence-sensitive evaluation environments. Wu et al. [25] introduced Jensen–Shannon divergence measures for intuitionistic fuzzy sets and constructed a parametric intuitionistic fuzzy TOPSIS to improve distance measurement and ranking accuracy. Xu and Lan [27] proposed an MCDM method combining intuitionistic fuzzy entropy with a three-way ranking TOPSIS model, offering more informative classifications in complex decision scenarios. Similarly, Masmali et al. [13] developed a TOPSIS method integrated with intuitionistic fuzzy soft sets, demonstrating improved accuracy in ovarian cancer diagnosis.

Neutrosophic theory, developed by Smarandache [20], [21], offers a more comprehensive structure by explicitly representing truth, indeterminacy, and falsity simultaneously. This theoretical foundation has motivated numerous applications in cyber-risk assessment. Abdel-Basset et al. [1] proposed a neutrosophic MCDM methodology for evaluating cybersecurity risks in power management systems, demonstrating enhanced modelling of inconsistent evidence. Similarly, Ismail et al. [8] introduced a neutrosophic measure-integral framework integrated with artificial intelligence, contributing to more robust cybersecurity solutions. Further, Santander Moreno et al. [18] developed a neutrosophic evaluation model for assessing information system security measures, highlighting the adaptability of neutrosophic representations to enterprise-level environments. In the context of IoT security, Khaled et al. [10] presented a neutrosophic neural network model capable of detecting cyber-attacks in highly uncertain network conditions.

Within the MCDM domain, numerous studies have extended classical TOPSIS frameworks into various neutrosophic and generalized environments. Zulqarnain et al. [28] formulated an integrated neutrosophic TOPSIS method, while Muhiuddin et al. [15] explored TOPSIS under bipolar quadripartitioned neutrosophic settings. Ucak Ozkaya [24] demonstrated the efficiency of hybrid N-AHP–TOPSIS models in evaluating biological and chemical alternatives, thereby validating the broader potential of neutrosophic MCDM approaches. Likewise, Manpreet Kaur and Singh [12] employed generalized neutrosophic TOPSIS within picture hyper-soft set structures, enabling decision-making in scenarios involving hierarchical and multi-valued criteria.

Almotiri [2] proposed a fuzzy TOPSIS method for evaluating network resilience under DDoS attacks, demonstrating the importance of integrating uncertainty-aware decision systems. Kumar [11] reviewed emerging cyber threats, emphasizing the necessity of adaptive modelling tools. More recently, Sarker [19] examined the impact of generative AI on cybersecurity, identifying novel threats such as adversarial AI attacks and automated exploitation pipelines, further reinforcing the need for decision frameworks capable of handling dynamic and indeterminate cyber landscapes. Soner [22] utilized fuzzy cognitive maps to analyze cybersecurity risk propagation in port environments, showing how causal threat interactions determine overall system vulnerability. Alsughayyir and Alsager [3] introduced a Multi-Q Valued Bipolar Picture Fuzzy Set model to represent complex bipolar and neutral assessments in cybersecurity risk evaluation.

Computational tools also play a crucial role in operationalizing advanced decision models. Sunil Rawan [23] highlighted MATLAB as a comprehensive environment for numerical computation and algorithmic implementation, making it well-suited for developing MCDM and neutrosophic-based threat evaluation systems.

Recent advancements have further expanded neutrosophic modelling capability. Boobalan and Mathivadhana introduced the NHSRM in [6], offering a unified structure capable of handling multi-attribute granularity and rough approximations simultaneously. Their subsequent work [7] established a determinant-theoretic model under NHSRM, evidencing the mathematical robustness of these matrices for complex MCDM tasks.

Integrating NHSRM with the TOPSIS further enhances decision-making capability in cybersecurity environments. TOPSIS ranks alternatives such as threat levels, suspicious sessions, compromised devices, or response actions based on their proximity to an ideal secure state and their distance from a worst-case attack state. When applied within NHSRM space, TOPSIS evaluates alternatives using neutrosophic truth, indeterminacy, and falsity components simultaneously, ensuring that ambiguity and conflict are preserved and properly weighted during decision computations rather than forced into simplified or binary judgments. As a result, the NHSRM-TOPSIS approach yields more realistic, interpretable, and robust rankings of cybersecurity alternatives compared to conventional crisp or single-valued fuzzy decision models.

1.2 Research gap

Although TOPSIS has been widely applied in fuzzy, intuitionistic fuzzy, and neutrosophic decision-making environments, existing studies predominantly rely on simplified neutrosophic matrices or aggregated single-layer uncertainty representations. These approaches often overlook the parameterized, multi-granular, and approximation-based structure inherent in real-world cybersecurity data, where uncertainty arises simultaneously from incomplete evidence, conflicting alerts, and indeterminate system states. However, the integration of TOPSIS within the NHSRM framework remains largely unexplored, particularly with respect to preserving the full neutrosophic structure during normalization, distance computation, and closeness coefficient evaluation. This reveals a clear research gap in developing a systematic NHSRM–TOPSIS methodology that maintains layered uncertainty and rough approximations while providing robust and interpretable rankings for cybersecurity decision-making problems.

1.3 Structure of the Proposed work

The structure of the proposed work is organized as follows:

- Section 2 presents the theoretical foundations, including the definitions of neutrosophic sets, hyper soft sets, NHSRMs, and their associated operations, properties, and mathematical preliminaries.
- Section 3 develops the complete decision-making framework: NHSRM construction, normalization, weighted matrix formulation, determination of Positive and Negative Ideal Solutions (PIS/NIS), and computation of closeness coefficients. This section also demonstrates the application of the proposed framework to cybersecurity threat prioritization by ranking malware, phishing, DDoS, and insider threats, along with a detailed sensitivity analysis under varying criteria weights.
- Section 4 presents the MATLAB-based algorithm implementing the proposed NHSRM–TOPSIS methodology.
- Section 5 summarizes the main findings, highlights the key contributions, and outlines potential directions for future research.

2. Preliminaries

This section presents the fundamental concepts of neutrosophic sets, NHSRM, and their relevant extensions that form the mathematical foundation of the proposed methodology.

Definition 2.1. [20]

Let E be a universe. A Neutrosophic set U on E can be defined as $U=\left\{\left\langle e,T^{U}(e),I^{U}(e),F^{U}(e)\right\rangle : e\in E\right\}$ where $T^{U}(e),I^{U}(e),F^{U}(e):E\rightarrow[0,1]$ denote the truth-membership, indeterminacy-membership and falsity-membership functions satisfying the condition $0\leq T^{U}(e)+I^{U}(e)+F^{U}(e)\leq 3$.

Definition 2.2. [9]

Consider a universe of discourse E with P(E) representing the set of all its possible subsets. Let $A_1, A_2, ..., A_\beta$ be the collection of well-defined attributes, $\beta \geq 1$, where each attribute A_i is associated with a finite set of attribute values $A_i^{q_i}$, $q_i \in 1,2,...,m_i$ for $i = 1,2,...,\beta$. The collection of all multi-parametric combinations of these refined values forms the product $A_1^{q_1} \times A_2^{q_2} \times .... \times A_\beta^{q_\beta}$. A neutrosophic hyper soft set relative to E is a pair $(\varphi, A_1^{q_1} \times A_2^{q_2} \times .... \times A_\beta^{q_\beta})$ where $\varphi : (A_1^{q_1} \times A_2^{q_2} \times .... \times A_\beta^{q_\beta}) \to P(E)$ and $\varphi(A_1^{q_1} \times A_2^{q_2} \times .... \times A_\beta^{q_\beta}) = \{\langle e, T^\lambda(e), I^\lambda(e), F^\lambda(e)\rangle \in E, \lambda \in (A_1^{q_1} \times A_2^{q_2} \times .... \times A_\beta^{q_\beta})\}$. Here, $T^\lambda(e)$, $I^\lambda(e)$ and $F^\lambda(e)$ represent the degrees of truth-membership, indeterminacy-membership and falsity-membership function respectively. If $U_{ij} = \vartheta(e_i, A_j^k)$, $i = 1,2,3,...,\alpha, j = 1,2,3,...,\beta$ and $k = q_1, q_2, q_3, ..., q_\beta$ then the corresponding Neutrosophic Hyper Soft Matrix can be expressed as

$$[U_{ij}]_{\alpha \times \beta} = \begin{bmatrix} U_{11} & U_{12} & ... & U_{1\beta} \\ U_{21} & U_{22} & ... & U_{2\beta} \\ \vdots & \vdots & \ddots & \vdots \\ U_{\alpha 1} & U_{\alpha 2} & ... & U_{\alpha\beta} \end{bmatrix}$$

where $U_{ij} = (T^{A_j^k}(e_i), I^{A_j^k}(e_i), F^{A_j^k}(e_i), e_i \in U, A_j^k \in (A_1^{q_1} \times A_2^{q_2} \times .... \times A_\beta^{q_\beta})) = (T_{ij}^U, I_{ij}^U, F_{ij}^U)$

Definition 2.3. [6]

Let $E = \{e_1, e_2, ..., e_\alpha\}$ be an non-empty universe set and P(E) be the set of all neutrosophic sets over E. Let U be the set of parameters, $U = \{A_1, A_2, ...A_n\}$, where $A_i \bigcap A_j = \varnothing \; for \; i \neq j$ Let $S_j \subseteq A_j, j \in \{1,2,...,n\}$ then then $\prod_{j=1}^n S_j^k \subseteq \prod_{j=1}^n A_j^k$. The pair $(\varphi, \prod_{j=1}^n S_j^k) = P(E)$, where φ is a mapping defined by $\varphi : \prod_{j=1}^n S_j^k \to P(E)$ is called neutrosophic hyper soft rough set. Each element $e \in E$ is associated with the values determined by the hyper soft set, where each parameter can take multiple values. For each element $e \in E$ related with a parameter A_j is represented by the triplet (T_{ij}, I_{ij}, F_{ij}) where T_{ij} is the truth membership function, I_{ij} is the indeterminacy membership function and F_{ij} is the falsity membership function, $T_{ij}, I_{ij}, F_{ij} \in [0,1]$.

If $U_{ij} = \gamma(u_i, A_j^k)$, where $i = i,2,3,...,\alpha, j = 1,2,3,...,\beta$ and $k = a,b,c,...,z$ then a NHSRM is defined as

$$U = \begin{bmatrix} <\underline{U}_{11}; \overline{U}_{11}> & <\underline{U}_{12}; \overline{U}_{12}> & ... & <\underline{U}_{1n}; \overline{U}_{1n}> \\ <\underline{U}_{21}; \overline{U}_{21}> & <\underline{U}_{22}; \overline{U}_{22}> & ... & <\underline{U}_{2n}; \overline{U}_{2n}> \\ \vdots & \vdots & \ddots & \vdots \\ <\underline{U}_{n1}; \overline{U}_{n1}> & <\underline{U}_{n2}; \overline{U}_{n2}> & ... & <\underline{U}_{nn}; \overline{U}_{nn}> \end{bmatrix}$$

Lower Approximation matrix is denoted by $\underline{U}_{ij} = (\underline{T}_{ij}^U, \underline{I}_{ij}^U, \underline{F}_{ij}^U)$, $0 \leq \underline{T}_{ij}^U + \underline{I}_{ij}^U + \underline{F}_{ij}^U \leq 3$ and

Upper Approximation matrix is denoted by $\overline{U}_{ij} = (\overline{T}_{ij}^U, \overline{I}_{ij}^U, \overline{F}_{ij}^U)$, $0 \leq \overline{T}_{ij}^U + \overline{I}_{ij}^U + \overline{F}_{ij}^U \leq 3$

Definition 2.4.

The Positive Ideal Solution (PIS) is a hypothetical alternative that maximizes the desirable criteria and minimizes the undesirable criteria.

$$\hat{D}_j^+ = \left(\max T_{ij}^{\hat{\theta}}, \max I_{ij}^{\hat{\theta}}, \min F_{ij}^{\hat{\theta}}\right)$$

The Negative Ideal Solution (NIS) is a hypothetical alternative that minimizes all desirable criteria and maximizes all undesirable criteria.

$$\hat{D}_j^- = \left(\min T_{ij}^{\hat{\theta}}, \min I_{ij}^{\hat{\theta}}, \max F_{ij}^{\hat{\theta}}\right)$$

3. Mathematical Formulation of TOPSIS-based MCDM Model in NHSRM

Definition 3.1.
Cybersecurity in the NHSRM framework refers to the systematic representation, analysis, and evaluation of cyber-threats, evidential sources, and security states under conditions of uncertainty, indeterminacy, and inconsistency. An NHSRM provides a multidimensional decision structure in which each cyber-entity (e.g., threats, alerts, logs, or sensor outputs) is modeled using neutrosophic triples capturing the degrees of truth, indeterminacy, and falsity across multiple parameter layers and sub-attributes, as permitted by the hyper-soft structure.

Remark 3.1.

- m alternatives (e.g., possible threat levels, sessions, devices, or actions)
- n attributes (e.g., severity, anomaly score, frequency, user privilege, endpoint risk, etc.)
- Each attribute may have sub-attributes, forming a hyper-soft environment.

Example 3.1. A 3×3 NHSRM $\hat{U}$ is expressed in the form

$$\hat{U} = \begin{bmatrix} \langle(0.7,0.3,0.1);(0.5,0.2,0.1)\rangle & \langle(0.8,0.5,0.4);(0.6,0.3,0.1)\rangle & \langle(0.5,0.3,0.2);(0.5,0.4,0.0)\rangle \\ \langle(0.6,0.2,0.1);(0.5,0.3,0.2)\rangle & \langle(0.8,0.4,0.3);(0.9,0.0,0.4)\rangle & \langle(1.0,0.3,0.2);(1.0,0.1,0.0)\rangle \\ \langle(1.0,0.2,0.1);(0.6,0.0,0.1)\rangle & \langle(0.9,0.4,0.1);(0.6,0.2,0.1)\rangle & \langle(0.7,0.5,0.3);(0.7,0.3,0.4)\rangle \end{bmatrix}$$

3.1 Algorithm

Step 1: Construct the decision NHSRM for all alternatives and criteria. $U = [U_{ij}], i = 1,2,...,m, j = 1,2,...,n$

Step 2: Calculate average approximation of the sub-attribute in each NHSRM entry is computed as $U = \left[\left\langle T_{ij}^U, I_{ij}^U, F_{ij}^U \right\rangle\right]$ where $T_{ij}^{\hat{\theta}} = \frac{\underline{T}_{ij}^{\hat{\theta}} + \bar{T}_{ij}^{\hat{\theta}}}{2}, I_{ij}^{\hat{\theta}} = \frac{\underline{I}_{ij}^{\hat{\theta}} + \bar{I}_{ij}^{\hat{\theta}}}{2}, F_{ij}^{\hat{\theta}} = \frac{\underline{F}_{ij}^{\hat{\theta}} + \bar{F}_{ij}^{\hat{\theta}}}{2}.$

Step 3: Normalize decision NHSRM by $\hat{N}_{ij} = \frac{\hat{U}_{ij}}{\sqrt{\sum_{i=1}^{m} \hat{U}_{ij}^2}}, j = 1,2,...,n$

Step 4: Apply criteria weights to the normalized Decision NHSRM $\hat{D}_{ij} = w_k.\hat{N}_{ij}$, where $\sum_{k=1}^{m} w_k = 1$

Step 5: Determine PIS and NIS by using Definition 2.4.
Step 6: Compute the distance of each alternative from both PIS & NIS

$$\hat{W}_{ij}^+ = \sqrt{\sum_{j=1}^{n} \left(T_{ij} - T_j^+\right)^2 + \left(I_{ij} - I_j^+\right)^2 + \left(F_{ij} - F_j^+\right)^2},$$

$$\hat{W}_{ij}^- = \sqrt{\sum_{j=1}^{n} \left(T_{ij} - T_j^-\right)^2 + \left(I_{ij} - I_j^-\right)^2 + \left(F_{ij} - F_j^-\right)^2}$$

Step 7: Compute Closeness Coefficient for each alternative $\hat{y}_i = \frac{\hat{W}_i^-}{\hat{W}_i^+ + \hat{W}_i^-}$

where $0 \leq \hat{Y}_i \leq 1, i = 1,2,...,m$

Step 8: Rank alternatives in descending order based on their Closeness Coefficient $\hat{Y}_i$, highest is the best.

3.2. Application

Modern cybersecurity systems are required to continuously monitor and analyze massive volumes of heterogeneous security data generated from multiple sources, including firewalls, intrusion detection systems (IDS), malware scanners, endpoint telemetry, User Behavior Analytics(UBA), authentication logs, and cloud service monitoring tools. These security alerts are not only diverse in form but also vary significantly in reliability and completeness. Real-world cyber environments suffer from several challenges, such as encrypted network traffic, evolving adversarial tactics, false positives from signature-based systems, and unknown zero-day vulnerabilities. Conventional threat evaluation methods, mainly probabilistic or fuzzy models, fail to handle this multidimensional uncertainty where decisions depend on multiple attributes, contextual factors, and inconsistent sensor outputs. To address these limitations, NHSRM provides a robust mathematical structure capable of representing multi-attribute threat information along with its indeterminate and contradictory nature. NHSRM extends neutrosophic sets to allow:

- Modeling of multi-attribute threat characteristics using hyper-soft parameterization,
- Handling of rough boundary regions when evidence is ambiguous or partially known,
- Quantification of truth (T), indeterminacy (I), and falsity (F) components simultaneously for each threat-evidence relation.

In this research, the NHSRM model is employed to construct an intelligent cyber-threat analysis framework capable of aggregating, evaluating, and ranking threats using multi-source cybersecurity evidence under uncertainty. The focus of the study is on improving the quality and reliability of threat-prioritization decisions by handling indeterminacy, conflict, and incompleteness in security data.

In the proposed decision-making scenario, the cyber threats are treated as the alternatives to be evaluated, namely Malware (T1), Phishing (T2), DDos (T3), Insider Threat (T4). The evidence sources serve as criteria, including Firewall Alerts, IDS Alerts, Endpoint Telemetry, UBA. By combining these threats and criteria within TOPSIS-based MCDM method in NHSRM framework, this work aims to provide a robust and uncertainty-aware mechanism for ranking cyber threats and supporting effective decision-making.

- Integrate heterogeneous alert information,
- Capture uncertainty, conflicting evidence, and dynamic attack behavior,
- Compute a reliable ranking of threats,
- Support proactive and intelligent cyber defense decision-making.

Specifically, the proposed framework is designed to:

Step 1: Consider the decision NHSRM U of order $4' 4$ as shown in Table 1.

Table 1 NHSRM

Threats/Evidence Source	Firewall Alerts	IDS Alerts	Endpoint Telemetry	User Behavior Analytics
Malware (T1)	(0.70, 0.12, 0.18); (0.80, 0.10, 0.10)	(0.72, 0.10, 0.18); (0.78, 0.08, 0.14)	(0.60, 0.15, 0.25); (0.68, 0.11, 0.21)	(0.87, 0.07, 0.06); (0.93, 0.05, 0.02)
Phishing (T2)	(0.69, 0.15, 0.16); (0.77, 0.13, 0.10)	(0.80, 0.09, 0.11); (0.85, 0.05, 0.10)	(0.66, 0.10, 0.20); (0.71, 0.10, 0.19)	(0.84, 0.12, 0.04); (0.91, 0.08, 0.01)
DDos (T3)	(0.73, 0.08, 0.19); (0.80, 0.06, 0.14)	(0.68, 0.18, 0.14); (0.73, 0.15, 0.10)	(0.71, 0.11, 0.18); (0.77, 0.09, 0.16)	(0.89, 0.10, 0.01); (0.95, 0.05, 0.0)
Insider threat (T4)	(0.66, 0.17, 0.17); (0.74, 0.14, 0.12)	(0.77, 0.13, 0.10); (0.81, 0.11, 0.08)	(0.69, 0.16, 0.15); (0.74, 0.13, 0.13)	(0.86, 0.09, 0.05); (0.92, 0.06, 0.02)

Step 2: The average approximation of the sub-attribute in each NHSRM $\hat{U}_{ij}$ is computed as shown in Table 2.

Table 2 Average Approximation NHSRM

Threats/Evidence Source	Firewall Alerts	IDS Alerts	Endpoint Telemetry	User Behavior Analytics
Malware (T1)	(0.75, 0.11, 0.14)	(0.75, 0.09, 0.16)	(0.64, 0.13, 0.23)	(0.90, 0.06, 0.04)
Phishing (T2)	(0.73, 0.14, 0.13)	(0.825, 0.07, 0.105)	(0.68, 0.10, 0.195)	(0.875, 0.10, 0.025)
DDos (T3)	(0.765, 0.07, 0.165)	(0.705, 0.165, 0.12)	(0.74, 0.10, 0.17)	(0.92, 0.075, 0.005)
Insider threat (T4)	(0.70, 0.155, 0.145)	(0.79, 0.12, 0.09)	(0.715, 0.145, 0.14)	(0.89, 0.075, 0.035)

Step 3: Normalize decision NHSRM as presented in Table 3.

Table 3 Normalize Decision NHSRM

Threats/Evidence Source	Firewall Alerts	IDS Alerts	Endpoint Telemetry	User Behavior Analytics
Malware (T1)	(0.509, 0.446, 0.481)	(0.487, 0.385, 0.658)	(0.459, 0.54, 0.616)	(0.502, 0.381, 0.678)
Phishing (T2)	(0.495, 0.568,0.446)	(0.536, 0.299, 0.432)	(0.492, 0.415, 0.522)	(0.488, 0.634, 0.424)
DDos (T3)	(0.519, 0.284, 0.566)	(0.458, 0.706, 0.493)	(0.532, 0.415, 0.455)	(0.513, 0.475, 0.084)
Insider threat (T4)	(0.475, 0.629, 0.498)	(0.514, 0.513, 0.37)	(0.514, 0.603, 0.375)	(0.496, 0.476, 0.594)

Step 4: Apply criteria weights to the normalized Decision NHSRM. Assume weights $w = (0.4, 0.3, 0.2, 0.1)$ for the four criteria cost [1,1,1,1], as shown in Table 4.

Table 4 Weight Normalize Decision NHSRM

Threats/Evidence Source	Firewall Alerts	IDS Alerts	Endpoint Telemetry	User Behavior Analytics
Malware (T1)	(0.20, 0.178, 0.192)	(0.146, 0.116, 0.197)	(0.092, 0.108, 0.123)	(0.05, 0.038, 0.068)
Phishing (T2)	(0.198, 0.227, 0.178)	(0.161, 0.09, 0.13)	(0.984, 0.083, 0.104)	(0.049, 0.063, 0.042)
DDos (T3)	(0.207, 0.114, 0.227)	(0.138, 0.212, 0.148)	(0.106, 0.831, 0.091)	(0.051, 0.047, 0.008)
Insider threat (T4)	(0.19, 0.252, 0.199)	(0.154, 0.154, 0.111)	(0.103, 0.121, 0.075)	(0.09, 0.047, 0.059)

Step 5: The PIS and NIS are determined using Definition 2.4, as shown in Table 5 and Table 6.

Table 5 PIS

$\mathcal{C}_j^+$	Malware (T1)	Phishing (T2)	DDos (T3)	Insider Threat (T4)
T_j^+	0.207	0.161	0.106	0.051
I_j^+	0.252	0.212	0.121	0.063
F_j^+	0.178	0.111	0.075	0.009

Table 6 NIS

$\mathcal{C}_j^-$	Malware (T1)	Phishing (T2)	DDos (T3)	Insider Threat (T4)
T_j^-	0.19	0.138	0.092	0.049
I_j^-	0.114	0.09	0.083	0.038

F_j^-	0.227	0.197	0.123	0.068

Step 6: The distance of each threat from both PIS and NIS are presented in Table 7 and Table 8.

Table 7 Distance of PIS

Threats	$\overset{o}{W}_{ij}^+$
Malware (T1)	0.171
Phishing (T2)	0.139
DDos (T3)	0.159
Insider threat (T4)	0.084

Table 8 Distance of NIS

Threats	$\overset{o}{W}_{ij}^-$
Malware (T1)	0.083
Phishing (T2)	0.149
DDos (T3)	0.150
Insider threat (T4)	0.189

Step 7: The Closeness Coefficient $\overset{o}{Y}_i$ for each threat is shown in Table 9.

Table 9 Closeness Coefficient

Threats	$\overset{o}{Y}_i$
Malware (T1)	0.327
Phishing (T2)	0.517
DDos (T3)	0.486
Insider threat(T4)	0.693

Step 8: Rank alternatives in descending order based on their Closeness Coefficient $\overset{o}{Y}_i$, as shown in Table 10 and Figure 1.

Table 10 Rank of Closeness Coefficient

Threats	$\overset{o}{y}_i$	Rank
Insider threat (T4)	0.693	1
Phishing (T2)	0.517	2
DDos (T3)	0.486	3
Malware (T1)	0.327	4

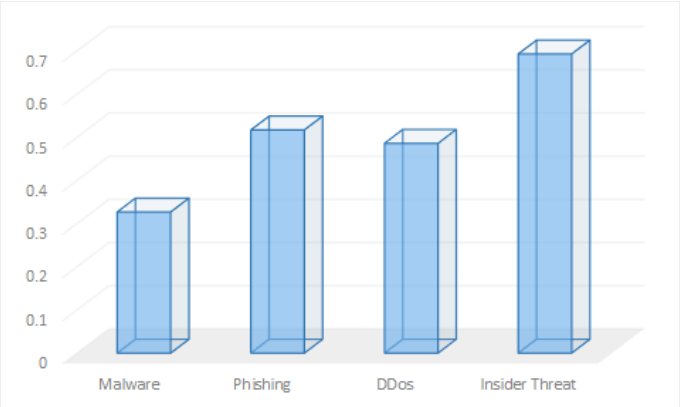

Figure 1: Rank of Closeness Coefficient $\overset{o}{Y}_i$

3.3 Sensitivity Analysis

A sensitivity analysis was performed using four different weighting scenarios (S1-S4) are shown in Table 11 and Figure 2 in order to examine the importance of security evidence sources (Firewall, IDS, Endpoint Telemetry,

UBA) influences the final ranking of threats. The stability index, presented in the Table 12, quantifies the robustness of these rankings across the scenarios. Based on this index, an overall cyber risk ranking of threats is established, providing a consistent and reliable assessment of the cybersecurity environment.

Table 11 Sensitivity Analysis

Scenario	Weight	Malware (T1)	Phishing (T2)	DDos (T3)	Insider threat (T4)	Rank
S1	(0.4, 0.3, 0.2, 0.1)	0.327	0.517	0.486	0.693	T4>T2>T3>T1
S2	(0.25, 0.25, 0.25, 0.25)	0.224	0.478	0.619	0.515	T3>T4>T2>T1
S3	(0.35, 0.35, 0.15, 0.15)	0.277	0.483	0.558	0.631	T4>T3>T2>T1
S4	(0.20, 0.20, 0.30, 0.30)	0.197	0.476	0.653	0.463	T3>T2>T4>T1

Table 12 Overall Cyber risk ranking by stability index

Final Stable Priority	Threat
Insider threat (T4)	Most frequently highest ranked; severe impact
DDos (T3)	Multiple Rank-1 results; high availability impact
Phishing (T2)	Medium but persistent rank
Malware (T1)	Lowest risk in all scenarios

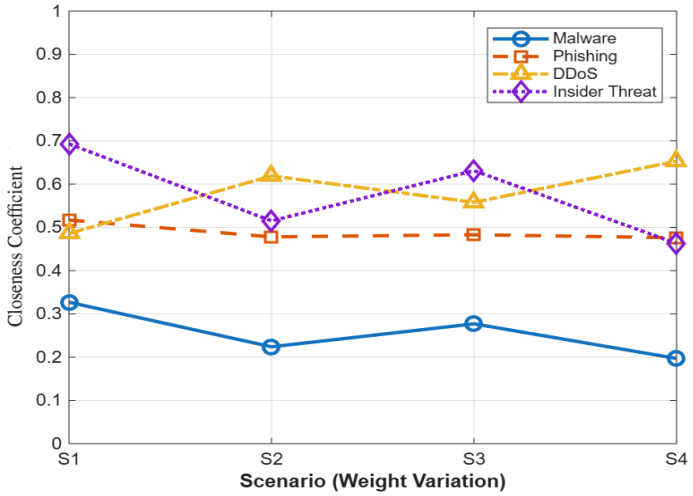

Figure 2: Sensitivity Analysis of Threat Ranking

4. MATLAB Code for TOPSIS-based MCDM Model in NHSRM

This section provides the complete MATLAB implementation of the proposed TOPSIS-based MCDM model within the NHSRM framework. The code automates all computational stages, including NHSRM construction, normalization, weight integration, PIS/NIS determination, final threat ranking, and the sensitivity analysis performed across multiple weighting scenarios.

4.1 Algorithm-1 TOPSIS-Based MCDM Model

Step1: Input NHSRM

Input m ← number of alternatives

Input n ← number of criteria

Input Tl (m×n) // Lower approximation Truth matrix

Input Tu (m×n) // Upper approximation Truth matrix

Input Il (m×n) // Lower approximation Indeterminacy matrix

Input Iu (m×n) // Upper approximation Indeterminacy matrix

Input Fl (m×n) // Lower approximation Falsity matrix

Input Fu (m×n) // Upper approximation Falsity matrix

Input w (1×n) // Weight vector of criteria

Input criteria (1×n) // 1 = benefit, 0 = cost

Step 2: Compute Average Approximations

For each i = 1 to m, j = 1 to n do

T(i,j) ← (Tl(i,j) + Tu(i,j)) / 2

I(i,j) ← (Il(i,j) + Iu(i,j)) / 2

F(i,j) ← (Fl(i,j) + Fu(i,j)) / 2

End for

Step 3: Normalization (Vector normalization)

For each criterion j = 1 to n do

Tnorm(:,j) ← T(:,j) / sqrt(sum(T(:,j).^2));

Inorm(:,j) ← I(:,j) / sqrt(sum(I(:,j).^2));

Fnorm(:,j) ← F(:,j) / sqrt(sum(F(:,j).^2));

End for

Step 4: Apply Weights

For each i = 1 to m, j = 1 to n do

Tw(i,j) ← Tnorm(i,j) * w(j)

Iw(i,j) ← Inorm(i,j) * w(j)

Fw(i,j) ← Fnorm(i,j) * w(j)

End for

Step 5: PIS and NIS

For each criterion j = 1 to n do

If criteria(j) = 1 (Benefit) then

Tplus(j) ← max(Tw(:,j))

Tminus(j) ← min(Tw(:,j))

Iplus(j) ← max(Iw(:,j))

Iminus(j) ← min(Iw(:,j))

Fplus(j) ← min(Fw(:,j))

Fminus(j) ← max(Fw(:,j))

Else (Cost)

Tplus(j) ← min(Tw(:,j))

Tminus(j) ← max(Tw(:,j))

Iplus(j) ← min(Iw(:,j))

Iminus(j) ← max(Iw(:,j))

Fplus(j) ← max(Fw(:,j))

Fminus(j) ← min(Fw(:,j))

End if

End for

Step 6: Distances

For each alternative i = 1 to m do

\Omega plus(i) ← sqrt(sum((Tw(i,:)-Tplus(j))^2

+ (Iw(i,:)-Iplus(j))^2 + (Fw(i,:)-Fplu(j)s)^2));

\Omega minus(i) ← sqrt(sum((Tw(i,:)-Tminus(j))^2

+ (Iw(i,:)-Iminus(j))^2 + (Fw(i,:)-Fminus(j))^2));

end

Step 7: Closeness Coefficient

For each alternative i = 1 to m do

\Psi(i) ← Dminus(i) / (\Omega plus(i) + \Omega minus(i))

End for

Step 8: Ranking

Assign ranks based on sorted \Psi values

Output final ranking of alternatives

4.2 Algorithm 2-Sensitivity Analysis on Closeness Coefficients

Step 1: Input Closeness Coefficient values

Display message:

"Sensitivity Analysis for Cyber Threat Prioritization"

Input number of scenarios: numScenarios

Initialize matrix \Psi of size (4 x numScenarios)

For each scenario s = 1 to numScenarios do

Prompt user to enter closeness coefficients

Order: [Malware, Phishing, DDoS, Insider Threat]

Store values in column s of matrix \Psi

End for

Define threat labels:

threats = {Malware, Phishing, DDoS, Insider Threat}

Generate scenario labels:

scenarios = {S1, S2, ..., S_numScenarios}

Step 2: Line plot: closeness across scenarios

For each threat i = 1 to 4 do

Plot closeness coefficient \Psi(i, :)

against scenario index

End for

Set x-axis as Scenario (Weight Variation)

Set y-axis as Closeness Coefficient

Add legend for threats

Enable grid and display plot

Output:

Line plot showing sensitivity of threat rankings

across different scenarios

End

4.3 Result and Discussion

In this study, TOPSIS-based MCDM method in the NHSRM framework was applied to cybersecurity threat evaluation. Four major cyber threats, Malware, Phishing, DDoS, and Insider Threat are assessed against multiple heterogeneous security evidence sources. The final threat rankings is obtained from the analysis is illustrated in Figure 1. To analyze robustness and stability of the ranking results, a sensitivity assessment is performed by varying attribute weights over four distinct scenarios.

From the illustration, we observe that the prioritization of cyber threats is highly sensitive to the assigned criteria weights, as depicted in Figure 2. When greater emphasis is placed on behavioral monitoring and firewall-based evidence (Scenarios S1 and S3), Insider Threat consistently emerges as the most critical cybersecurity risk.

Conversely, when equal weights are assigned or higher importance is given to IDS and endpoint telemetry evidence (Scenarios S2 and S4), DDoS is ranked as the top-priority threat. Across all scenarios, Malware consistently ranks as the least significant threat, reflecting the relative maturity and effectiveness of existing malware defense mechanisms, whereas Phishing remains a moderate risk regardless of weight variations. These results demonstrate that the NHSRM–TOPSIS model effectively captures uncertainty, conflicting evidence, and heterogeneous alert information, thereby providing a flexible and explainable framework for cyber-threat prioritization. As a final outcome, the analysis confirms that Insider Threats and DDoS attacks constitute the most critical risks under varying operational conditions, underscoring the necessity for adaptive weighting strategies and targeted defense planning in dynamic cybersecurity environments.

5. Conclusion

In this research, TOPSIS-Based MCDM in the NHSRM framework was developed and implemented using MATLAB to evaluate and rank cyber threats under uncertainty. The proposed approach is capable of processing heterogeneous and indeterminate evidence collected simultaneously from multiple monitoring sources such as firewalls, IDS, endpoint systems, and user-behavior analytics. Experimental results confirm that the model effectively prioritizes threats while preserving the inherent uncertainty and conflicts in security data. Furthermore, the sensitivity analysis demonstrates that threat rankings depend significantly on the assigned evidence-source weights. In particular, Insider Threat and DDoS consistently appear as dominant risk categories across multiple weight configurations. This highlights the operational importance of periodically revisiting and tuning weight assignments based on evolving attack patterns and organizational priorities. The proposed model provides a practical and flexible decision-support tool that enhances cyber-risk assessment and helps optimize incident response actions.

Future research can focus on large-scale real-time deployments, automatic weight adaptation using threat intelligence feeds, and comparative analysis with other neutrosophic decision-making approaches to further enhance resilience and responsiveness in cybersecurity operations.

Acknowledgements

The authors would like to express their sincere gratitude to all individuals and institutions that contributed to the successful completion of this research. Their guidance, support, and constructive feedback were invaluable throughout the study.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Abdel-Basset, M., Mohamed, R., & Elzein, I. (2023). Neutrosophic MCDM Methodology for Assessment Risks of Cyber Security in Power Management. Neutrosophic Systems with Applications, 9, 30-46. https://doi.org/10.61356/j.nswa.2023.11

[2] Almotiri, Sultan H. "Improving network resilience against DDoS attacks: A fuzzy TOPSIS-based quantitative assessment approach." Heliyon 10, no. 22 (2024). https://doi.org/10.1016/j.heliyon.2024.e40413

[3] Alsughayyir, N. M., & Alsager, K. M. (2025). A Novel Multi-Q Valued Bipolar Picture Fuzzy Set Approach for Evaluating Cybersecurity Risks. Symmetry, 17(5), 749. https://doi.org/10.3390/sym17050749

[4] Atanassov, K.T.: Intuitionistic fuzzy sets. Fuzzy Sets Syst. 20, 87–96 (1986)

[5] Bhowmik, A., Mandal, P., Samanta, S., Pal, M., & Allahviranloo, T. (2024). TOPSIS-Based MAGDM Under Linguistic Z Number Information. In Management of Uncertainty Using Linguistic Z-Numbers: Applications for Decision-Making, Granular Computing and Social Networks (pp. 17-31). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65854-9 2

[6] Boobalan, J., & Mathivadhana, E. (2025). An Approach to Neutrosophic Hyper Soft Rough Matrix and its Application. Neutrosophic Sets and Systems, 85, 305-328. https://doi.org/10.5281/zenodo.15265783

[7] Boobalan, J., & Mathivadhana, E. (2026). Determinant-Theoretic Model for MCDM under Neutrosophic Hyper Soft Rough Matrices. Neutrosophic Sets and Systems, 95, 229-263. https://doi.org/10.5281/zenodo.17088746

[8] Ismail, Mahmoud M., Ahmed A. Metwaly, Osama ElKomy, Alaa Al-Ghamry, and Eman Sayed. (2025). "Neutrosophic Measure-Integral Model for Advanced Cybersecurity Solutions Using Artificial Intelligence and Soft Computing Technique." Neutrosophic Sets and Systems 93: 711-726. https://doi.org/10.5281/zenodo.17167275

[9] Jayasudha, J., \& Raghavi, S. (2024). Some Operations on Neutrosophic Hypersoft Matrices and Their Applications. Neutrosophic Systems with Applications, 21, 46-62. https://doi.org/10.61356/j.nswa.2024.21354

[10] Khaled, O. M., A. A. Salama, Mostafa Herajy, M. M. El-Kirany, Huda E. Khalid, Ahmed K Essa, and Ramiz Sabbagh. (2025). "A Novel Approach for Cyber-Attack Detection in IoT Networks with Neutrosophic Neural Networks." Neutrosophic Sets and Systems 86, no. 1: 48. https://doi.org/10.5281/zenodo.15540377

[11] Kumar, I. (2023). Emerging Threats in Cybersecurity: A Review Article. International Journal of Applied and Natural Sciences, 1(1), 01–08.

[12] Manpreet Kaur, & Akanksha Singh. (2024). Approach to Multi-Criteria Decision-Making in a Neutrosophic Picture Hyper-Soft Set Environment using Generalized Neutrosophic TOPSIS. Neutrosophic Sets and Systems, 67, 75-104. https://doi.org/ 10.5281/zenodo.11123590

[13] Masmali, I., Ahmad, A., Azeem, M., Koam, A. N., & Alharbi, R. (2024). TOPSIS method based on intuitionistic fuzzy soft set and its application to diagnosis of ovarian cancer. International Journal of Computational Intelligence Systems, 17(1), 161. https://doi.org/10.1007/s44196-024-00537-1

[14] Molodtsov, D. (1999) Soft Set Theory—First Results. Computers & Mathematics with Applications, 37, 19-31. http://dx.doi.org/10.1016/S0898-1221(99)00056-5

[15] Muhiuddin, G., Mohamed E. Elnair, Satham Hussain S, & Durga Nagarajan. (2025). TOPSIS method-based decision-making model for bipolar quadripartitioned neutrosophic environment. Neutrosophic Sets and Systems, 85, 899-918. https://doi.org/ 10.5281/zenodo.15399451

[16] Pawlak, Z. (1982) Rough Sets. International Journal of Information and Computer Science, 11, 341-356. http://dx.doi.org/10.1007/BF01001956

[17] Sahoo, L., Senapati, T., Pal, M., & Yager, R. R. (Eds.). (2025). Decision Making Under Uncertainty Via Optimization, Modelling, and Analysis. Springer.

[18] Santander Moreno, J. J., Ortega Matoma, J. A., Raúl Dávila Castillo, M., & Ordóñez Sarchi, J. A. (2024). A neutrosophic framework for evaluating security measures in information systems. Journal of fuzzy extension and applications, 5(Spec. Issue), 12-29. https://doi.org/10.22105/jfea.2024.468184.1546

[19] Sarker, I. H. (2025). Generative AI revolution in cybersecurity: a comprehensive review of threats, risks, and solutions. Artificial Intelligence Review, 58(5), 1-40. https://doi.org/10.1007/s10462-025-11219-5

[20] Smarandache, F. (2015). Symbolic neutrosophic theory. Infinite Study.

[21] Smarandache, F. (2021). Practical Applications of the Independent Neutrosophic Components and of the Neutrosophic Offset Components. Infinite Study.

[22] Soner, O. (2025). Modeling and analyzing cybersecurity risk propagation in ports using fuzzy cognitive maps: System sensitivity to key threat factors. Ocean & Coastal Management, 270,107857.

[23] Sunil Rawan, (2025). MATLAB: A Comprehensive Platform for Scientific Computing and Engineering Applications. Journal of Emerging Technologies and Innovative Research 12(7), d528-d536. https://doi.org/10.56975/jetir.v12i7.566477

[24] Ucak Ozkaya, Gulsum. (2025). A Hybrid N-AHP-Based TOPSIS Decision Support Approach for Investigation of the Effect of Different Solvents on the Bioactive Properties, Anticancer, and Antimicrobial Activities of Aronia melanocarpa Extract. Food Science & Nutrition 13, no. 4: e70122. https://doi.org/10.1002/fsn3.70122

[25] Wu, X., Liu, Q., Liu, L., Yang, M. S., & Zhang, X. (2025). New Jensen‐Shannon divergence measures for intuitionistic fuzzy sets with the construction of a parametric intuitionistic fuzzy TOPSIS. Complex and Intelligent Systems, 11(2), 134. https://doi.org/10.1007/s40747-024-01761-0

[26] Zadeh, L.A. (1965). Fuzzy sets. Inf. Control 8(3), 338–353.
[27] Xu, C., & Lan, Y. (2025). A Multi-criteria Decision-Making Method Based on Intuitionistic Fuzzy Entropy and Three-Way Ranking TOPSIS with Applications. International Journal of Fuzzy Systems, 1-24. https://doi.org/10.1007/s40815-024-01954-2
[28] Zulqarnain, R. M., Xin, X. L., Saqlain, M., Smarandache, F., & Ahamad, M. I. . (2021). An integrated model of Neutrosophic TOPSIS with application in Multi-Criteria Decision-Making Problem. Neutrosophic Sets and Systems, 40, 253-269.