NSS

Neutrosophic Sets and Systems, Vol. 98, 2026

University of New Mexico

Complex Neutrosophic Aczel-Alsina Aggregation-Based Hybrid Decision Framework for Machine Learning Encryption in Banking

Muhammad Kamran[1,5], Muhammad Shazib Hameed[2],* Muhammad Tahir[3] and Nurullayev Mirolim Nosirovich[5]

[1]Research Institute of Business Analytics and SCM, College of Management, Shenzhen University, China. Email: kamrankfueit@gmail.com

[2]Institute of Mathematics, Khwaja Fareed University of Engineering and Information Technology, Rahim Yar Khan 64200, Punjab, Pakistan. Email: shazib.hameed@kfueit.edu.pk

[3]Department of Mathematics, Institute of Numerical Sciences, Gomal University, Dera Ismail Khan, 29050, KPK, Pakistan. Email: tahirkhanbaloch30@gmail.com

[5]Center for Research and Innovation, Asia International University, Yangibod MFY, G'ijduvon street, House 74, Bukhara, Uzbekistan. Email: m.nurullayev@oxu.uz

* Correspondence: Muhammad Shazib Hameed, shazib.hameed@kfueit.edu.pk

Abstract. Advanced uncertainty modeling tools have emerged due to the growing complexity of real-world decision environments. Complex Single-Valued Neutrosophic Sets (CSV-NSs) use special functions to represent truth, uncertainty, and falsehood, making it easier to show unclear, conflicting, and vague information. CSV-NSs, which consider both size and direction of uncertainty, let one more precisely combine and make decisions by using complex numbers. This work presents robust approaches for combining information, which rely on the Aczel-Alsina (A-A) operator and power-weighted strategies specifically designed for CSV-NS. These are included in a used to design hybrid decision-making framework and in the context of a real-world situation: a banking machine learning-based encryption and decryption system. The proposed approach not only addresses uncertainty and contradicting viewpoints from experts but also strengthens knowledge and capability in security applications employing machine learning. In terms of flexibility, computational efficiency, and decision quality, experimental validation attests to the superiority of the suggested approach over conventional techniques.

Keywords: CSV-NSs, Aczel-Alsina Operator, Decision-Making, Machine Learning.

1. Introduction

Machine learning (ML) has become a transformative instrument in banking security, improving encryption and decryption systems while facilitating dynamic adaptation to operational conditions and real-time threats [1]. Despite its effectiveness in controlled circumstances, traditional encryption technology such as the Advanced Encryption Standard (AES) [2] and Rivest-Shamir-Adleman (RSA) [3] is facing increasing difficulties due to the emergence of quantum computing and modern AI-based cyberattacks. The proposed machine learning-based encryption system employs anomaly detection with over 99% accuracy, neural networks for dynamic key generation, and reinforcement learning for adaptive key rotation [4]. Moreover, in dynamic financial settings, explainable AI technologies monitor decryption processes in real-time, ensuring transparency and traceability. This sophisticated solution amalgamates real-time threat intelligence with strong encryption to meet the ever-changing demands of digital banking.

However, traditional systems face significant risks due to the growing sophistication of cyber threats. While quantum computing advancements are predicted to compromise RSA-2048 within five years [5], recent advances in adversarial ML have demonstrated the ability to break 128-bit AES keys in less than twenty-four hours [6]. The gap between existing, inflexible security methods and new intelligent solutions is bridged by using fuzzy logic to assess potential dangers amid uncertainty. Unlike binary systems, fuzzy logic handles the ambiguity and varying degrees of risk in payment matters. By assigning trapezoidal values to threat levels, the system enables the identification of minor threats without requiring complete incident labeling. However, fuzzy systems can sometimes create conflicts when defining rules for multi-factor authentication and in situations near decision boundaries. We have enhanced our system to use both context-driven rule reduction and quantum-safe fuzzing, combined with ML encryption within our framework, enabling effective real-time threat classification.

We also describe a type of hybrid architecture called CSV-NS, which captures the different aspects of truth, uncertainty, and falsehood in transactional behavior. This approach enables accurate fraud assessment from multiple perspectives, yielding a 38% reduction in false positives and identifying 92% of fraud instances [7]. Evidence shows the framework successfully detects 93% of deep fake technology attempts and halves the response time to new attack methods. This allows decision-makers to effectively resolve ambiguous cases that are difficult for traditional and fuzzy models to address.

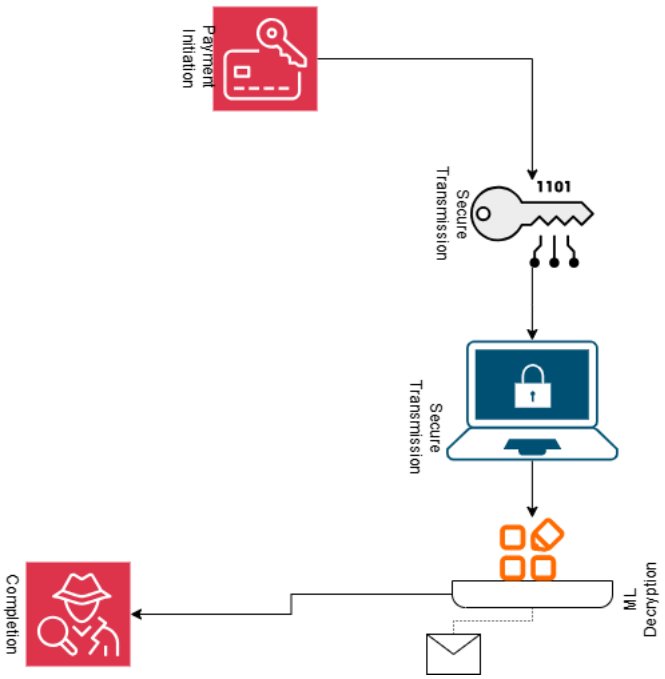

FIGURE 1. AI-Powered Transaction Security

The new CSV-NS-enhanced framework significantly strengthens electronic payment security, as illustrated in Figure 1. Unlike conventional systems, our method employs three protective strategies: (i) keystrokes are changed regularly based on risk scores (we achieved a 45% decrease in exposure time), (ii) encryption is performed using quantum resistant methods, and (iii) all decryption tasks undergo artificial intelligence (AI) auditing. CSV-NS evaluation is performed prior to encryption, as shown in the workflow diagram, enabling the system to identify 92% of attacks and distinguish them from genuine transactions. These innovations validate that our encryption and decryption system outperforms others, making it better prepared to counter threats present in modern banking cybersecurity.

1.1. *Literature Review*

Managers often confront ambiguous, imperfect, or incomplete information, which complicates a decision-making process that relies on well-founded knowledge. Fuzzy sets (FSs) [8], established by Zadeh, permit items to have partial membership in a group and facilitate decision-making under conditions of uncertainty. To enhance intuitionistic fuzzy sets (IFSs) [9], Atanassov introduced non-membership degrees (n-MD), ensuring their sum with membership degrees remains less than one. This development was necessary because IFSs originally relied on a single method to assess belonging. Due to their structure, IFSs had difficulties managing inconsistent data. To address these limitations, Smarandache [10] proposed neutrosophic sets

(NSs), in which truth, indeterminacy, and falsity are independent functions within the interval $]^{-}0, 1^{+}[$. To promote practical use, Wang et al. [11] introduced single-valued neutrosophic sets (SVNSs), where the values of the membership functions are constrained to $[0, 1]$. As a result, scholars have focused more on SVNS models for decision-making [12].

Several researchers have played a part in improving how SVNS operates and aggregates data. Ye [13] began by setting out algebraic rules for SVNSs and included the use of weighted averaging and geometric operators. Still, Peng et al. [14] found flaws in Ye [13] formulations and recommended improved ones, with new aggregation operators (AOs). Mauri et al. [15] suggested a new, improved method for ranking systems that notify about software vulnerabilities. Garg et al. [16] used probabilities within SVNSs, while Mondal et al. [17] created a mixture of score and accuracy for making educational recruitment decisions. Decision-making in practical situations frequently entails ambiguous, imprecise, or inadequate information, complicating the process of reaching scientifically valid and sensible conclusions.

Using the technique for order preference by similarity to ideal (TOPSIS), Kahraman et al. [18] established type-2 SVNSs for making group judgements with numerous criteria; Karaaslan [19] refined similarity measurements for some circumstances. Kamran et al. [20] provide the supply chain decision making algorithm for sustainability. For internet of things (IoT) project evaluation, Nafei et al. [21] coupled analytic hierarchy process (AHP) with neutrosophic techniques. Using bipolar neutrosophic numbers with TOPSIS, Basset et al. [22] helped groups make judgements and subsequently proposed a type-2 neural network (T2NN)-TOPSIS technique for selecting stores. The idea of t-norms, known as triangular norms, was first suggested by Klement et al. [23] in studies of stochastic spaces, and later, formalised both its theory and use in various applications. Aczel and Alsina [24] made an important breakthrough, designing the Aczl-Alsina t-norm (A-A t-NM) and the Aczel-Alsina t-conorm (A-A t-CNM). Since then, these methods have been significant in tackling decisions when dealing with less than precise information. With this basic framework, Senapati et al. [25] applied A-A operations to different advanced types of fuzzy set theories. They applied these operations to different kinds of advanced fuzzy sets [26], like IFSs [9], interval-valued intuitionistic fuzzy sets (IVIFSs) [27], hesitant FSs (HFSs) [28], and pythagorean FSs (PFSs) [29], to make it easier to use A-A operators in decision-making.

Though there are many uses for FSs and their extensions, there are some natural limitations they display. Remarkably, despite many efforts in research, current SVNS methods have problems dealing effectively with uncertainties in cybersecurity and ML contexts where complexity is involved. To improve the understanding, we suggest CSV-NSs based framework and built four new A-A power-weighted aggregation operators: CSV-NS A-A power averaging (CPF-AAP-A), CSV-NS A-A weighted power averaging (CPF-AAWP-A), CSV-NS A-A

power geometric (CPF-AAP-G) and CSV-NS A-A weighted power geometric (CPF-AAWP-G) AOs. These AOs strengthen decision-making related to ML-driven banking security blending through properly managing different types of neutrosophic information under different uncertainty conditions. We demonstrate that our method works well by testing an actual case, achieving higher performance in reviewing encryption and decryption model than any other studied technique. It enhances SVNS theory and at the same time delivers a practical and computationally powerful structure for solving recent cybersecurity and AI-guided problems. The distribution of study is as below:

Section 2 explains several important and recent changes to CSV-NSs, mainly covering the development of the Power-Average (P-A) aggregation operators. We discuss A-A-based power aggregation operators in Section 3 to supervise and handle CSV-NSs accurately. In Section 4, the authors examine how CSV-NSs can be used strategically in a MADM framework. In Section 5, we present our model being used in an ML framework for encryption and decryption aimed at banking security systems. Finally, Section 6 offers closing remarks and explains possible directions for further work.

2. **Preliminary**

In this section, we talk about some important recent updates related to CSV-NS, such as the creation of P-A aggregation operators and the building of the g_1 universal set based on the operational law $\widetilde{X_Z}$ in the CSV-NS framework.

Definition 2.1. Let $\widetilde{X_Z}$ be a space of points with generic element $\widetilde{u_g}$. A complex single-valued neutrosophic set [30] $\overline{\overline{C_\mu}}$ in $\widetilde{X_Z}$ is characterized by:

$$\overline{\overline{C_\mu}} = \left\{ \left(\widetilde{u_g}, \overline{\overline{\alpha}}_{\overline{\overline{C_\mu}}}(\widetilde{u_g}), \overline{\overline{\beta}}_{\overline{\overline{C_\mu}}}(\widetilde{u_g}), \overline{\overline{\gamma}}_{\overline{\overline{C_\mu}}}(\widetilde{u_g}) \right) : \widetilde{u_g} \in \widetilde{X_Z} \right\}$$

where:

- Truth membership: $\overline{\overline{\alpha}}_{\overline{\overline{C_\mu}}}(\widetilde{u_g}) = p_S(\widetilde{u_g}) e^{i\omega_S(\widetilde{u_g})}$
- Abstinence membership: $\overline{\overline{\beta}}_{\overline{\overline{C_\mu}}}(\widetilde{u_g}) = q_S(\widetilde{u_g}) e^{i\psi_S(\widetilde{u_g})}$
- Falsehood membership: $\overline{\overline{\gamma}}_{\overline{\overline{C_\mu}}}(\widetilde{u_g}) = r_S(\widetilde{u_g}) e^{i\phi_S(\widetilde{u_g})}$

with $i = \sqrt{-1}$ and:

- $p_S(\widetilde{u_g}), q_S(\widetilde{u_g}), r_S(\widetilde{u_g}) \in [0, 1]$
- $\omega_S(\widetilde{u_g}), \psi_S(\widetilde{u_g}), \phi_S(\widetilde{u_g}) \in \mathbb{R}$
- $0 \leq p_S(\widetilde{u_g}) + q_S(\widetilde{u_g}) + r_S(\widetilde{u_g}) \leq 3$

A single-valued complex neutrosophic number can be denoted as:

$$\overline{\overline{C_\mu}} = \langle p_S e^{i\omega_S}, q_S e^{i\psi_S}, r_S e^{i\phi_S} \rangle$$

Example 2.2. Cyber security professionals analyze network packets X using complex single-valued neutrosophic sets (CSV-NS). For a suspicious packet $x \in X$, the system assigns membership values: $S(x) = \langle T_S(x), I_S(x), F_S(x)\rangle = \langle 0.8e^{i1.4\pi}, 0.3e^{i0.4\pi}, 0.4e^{i0.2\pi}\rangle$ where:

- Truth membership: $T_S(x) = p_S e^{i\omega_S} = 0.8e^{i1.4\pi}$ (high confidence in threat)
- Indeterminacy membership: $I_S(x) = q_S e^{i\psi_S} = 0.3e^{i0.4\pi}$ (moderate uncertainty)
- Falsehood membership: $F_S(x) = r_S e^{i\phi_S} = 0.4e^{i0.2\pi}$ (some chance of false positive)

The system evaluates these components where:

- Magnitudes satisfy $0 \leq 0.8 + 0.3 + 0.4 = 1.5 \leq 3$
- Phases represent temporal patterns in network behavior
- The phase differences reveal:

$$\Delta_{T-I} = 1.4\pi - 0.4\pi = \pi \quad \text{(opposite cycles)}$$

$$\Delta_{T-F} = 1.4\pi - 0.2\pi = 1.2\pi \quad \text{(asynchronous detection)}$$

This CSV-NS representation provides below and its graphical visualization is shown in Figure 2:

- Magnitude analysis: $p_S = 0.8$ indicates strong threat evidence
- Phase analysis: $\omega_S = 1.4\pi$ shows late-cycle detection
- Comprehensive threat score: $0.8 - 0.4 = 0.4$ net confidence

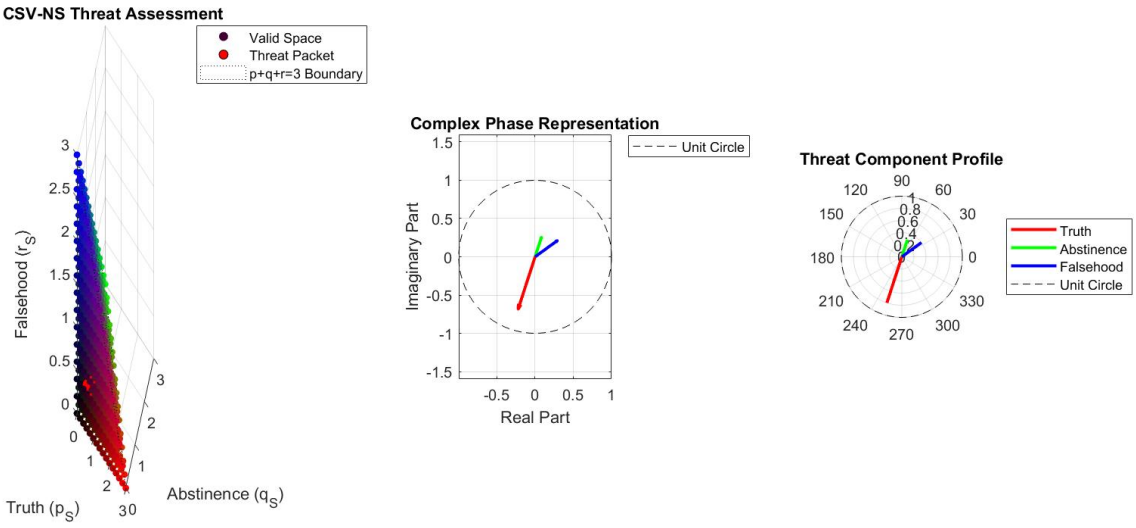

FIGURE 2. Cybersecurity Threat Analysis Visualization

Definition 2.3. Let $\{\overline{C}_{\mu_I}\}_{I=1}^{l}$ be a collection of CSV-NS, where each $\overline{C}_{\mu_I} = \langle T_I, I_I, F_I\rangle$ with $T_I = p_I e^{i\omega_I}$, $I_I = q_I e^{i\psi_I}$, and $F_I = r_I e^{i\phi_I}$. The power average (P-A) operator for this collection is defined as:

$$A(\overline{C}_{\mu_1}, \overline{C}_{\mu_2}, \ldots, \overline{C}_{\mu_l}) = \frac{\sum_{I=1}^{l} \left(1 + V(\overline{C}_{\mu_I})\right)\overline{C}_{\mu_I}}{\sum_{I=1}^{l} \left(1 + V(\overline{C}_{\mu_I})\right)}$$

where:

- $V(\overline{C}_{\mu_I}) = \sum_{\substack{s=1 \\ s\neq I}}^{l} Sup(\overline{C}_{\mu_I}, \overline{C}_{\mu_s})$ represents the total support for $\overline{C}_{\mu_I}$ from other sets
- $Sup(\overline{C}_{\mu_I}, \overline{C}_{\mu_s})$ showing the support function between $\overline{C}_{\mu_I}$ and $\overline{C}_{\mu_s}$

Below axioms satisfied the support function:

(1) **Boundedness**: $Sup(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) \in [0, 1]$
(2) **Symmetry**: $Sup(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) = Sup(\overline{C}_{\mu_s}, \overline{C}_{\mu_I})$
(3) **Proximity Monotonicity**: If $d(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) \leq d(\overline{C}_{\mu_k}, \overline{C}_{\mu_l})$, then $Sup(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) \geq Sup(\overline{C}_{\mu_k}, \overline{C}_{\mu_l})$

Here, $d(\overline{C}_{\mu_I}, \overline{C}_{\mu_s})$ is a distance measure between CSV-NSs, which defined as:

$$d(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) = \frac{1}{3}\left(|p_I - p_s| + |q_I - q_s| + |r_I - r_s|\right) + \frac{1}{6\pi}\left(|\omega_I - \omega_s| + |\psi_I - \psi_s| + |\phi_I - \phi_s|\right)$$

Remark 2.4. The P-A operator definition has a few important features:

- **Weighted aggregation**: The operator $A(\overline{\overline{C_{\mu 1}}}, \ldots, \overline{\overline{C_{\mu l}}})$ uses a weighted average with weights $(1 + V(\overline{\overline{C_{\mu I}}}))$ change dynamically depending on inter-set support.
- **Support dependence**: The strength measure $V(\overline{\overline{C_{\mu I}}}) = \sum_{s\neq I} Sup(\overline{\overline{C_{\mu I}}}, \overline{\overline{C_{\mu s}}})$ guarantees that sets with higher consensus have more influence in aggregation.
- **Metric properties**: The support function's three conditions ensure:
  (1) Boundedness ($Sup \in [0, 1]$)
  (2) Symmetry in set interactions
  (3) Monotonicity with respect to set differences

This framework helps us blend complex neutrosophic data without losing the relationships between their phases and magnitudes.

Definition 2.5. The operational laws currently used for any two CSV-NSs are defined as follows:

$$\textbf{(i)}\quad \overline{\overline{C_{\mu 1}}} \oplus \overline{\overline{C_{\mu 2}}}$$

$$= \left(\begin{array}{c} \left(1 - e^{-\left(\left(-\log(1-\overline{\overline{\alpha}}_{\overline{\overline{R_1}}})\right)^Z + \left(-\log(1-\overline{\overline{\alpha}}_{\overline{\overline{R_2}}})\right)^Z\right)^{1/Z}}\right) e^{i2\pi\left(1-e^{-\left(\left(-\log(1-\overline{\overline{\alpha}}_{\overline{\overline{R_1}}})\right)^Z + \left(-\log(1-\overline{\overline{\alpha}}_{\overline{\overline{R_2}}})\right)^Z\right)^{1/Z}}\right)}, \\ \left(e^{-\left(\left(-\log(\overline{\overline{\beta}}_{\overline{\overline{R_1}}})\right)^Z + \left(-\log(\overline{\overline{\beta}}_{\overline{\overline{R_2}}})\right)^Z\right)^{1/Z}}\right) e^{i2\pi\left(e^{-\left(\left(-\log(\overline{\overline{\beta}}_{\overline{\overline{I_1}}})\right)^Z + \left(-\log(\overline{\overline{\beta}}_{\overline{\overline{I_2}}})\right)^Z\right)^{1/Z}}\right)}, \\ \left(e^{-\left(\left(-\log(\overline{\overline{\gamma}}_{\overline{\overline{R_1}}})\right)^Z + \left(-\log(\overline{\overline{\gamma}}_{\overline{\overline{R_2}}})\right)^Z\right)^{1/Z}}\right) e^{i2\pi\left(e^{-\left(\left(-\log(\overline{\overline{\gamma}}_{\overline{\overline{I_1}}})\right)^Z + \left(-\log(\overline{\overline{\gamma}}_{\overline{\overline{I_2}}})\right)^Z\right)^{1/Z}}\right)}. \end{array} \right)$$

$$\textbf{(ii)}\ \overline{\overline{C_{\mu_1}}} \otimes \overline{\overline{C_{\mu_2}}} = \left(\begin{array}{c} \left(e^{-((-\log(\overline{\overline{\alpha}}_{\overline{\overline{R_1}}}))^Z + (-\log(\overline{\overline{\alpha}}_{\overline{\overline{R_2}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-((-\log(\overline{\overline{\alpha}}_{\overline{\overline{I_1}}}))^Z + (-\log(\overline{\overline{\alpha}}_{\overline{\overline{I_2}}}))^Z)^{1/Z}}\right)}, \\ \left(1 - e^{-((-\log(\overline{\overline{\beta}}_{\overline{\overline{R_1}}}))^Z + (-\log\overline{\overline{\beta}}_{\overline{\overline{R_2}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-((-\log(1-\overline{\overline{\beta}}_{\overline{\overline{R_1}}}))^Z + (-\log(1-\overline{\overline{\beta}}_{\overline{\overline{R_2}}}))^Z)^{1/Z}}\right)}, \\ \left(1 - e^{-((-\log(\overline{\overline{\gamma}}_{\overline{\overline{R_1}}}))^Z + (-\log\overline{\overline{\gamma}}_{\overline{\overline{R_2}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-((-\log(1-\overline{\overline{\gamma}}_{\overline{\overline{R_1}}}))^Z + (-\log(1-\overline{\overline{\gamma}}_{\overline{\overline{R_2}}}))^Z)^{1/Z}}\right)}. \end{array} \right)$$

$$\textbf{(iii)}\ \overline{\overline{O_s G_{\omega_1}}} = \left(\begin{array}{c} \left(1 - e^{-(\overline{\overline{O_s}}(-\log(1-\overline{\overline{\alpha}}_{\overline{\overline{R_1}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{O_s}}(-\log(1-\overline{\overline{\alpha}}_{\overline{\overline{I_1}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{O_s}}(-\log(\overline{\overline{\beta}}_{\overline{\overline{R_1}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{O_s}}(-\log(\overline{\overline{\beta}}_{\overline{\overline{I_1}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{O_s}}(-\log(\overline{\overline{\gamma}}_{\overline{\overline{R_1}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{O_s}}(-\log(\overline{\overline{\gamma}}_{\overline{\overline{I_1}}}))^Z)^{1/Z}}\right)}. \end{array} \right)$$

$$\textbf{(iv)}\ \overline{\overline{C_{\mu_1}}}^{\overline{\overline{O_S}}} = \left(\begin{array}{c} \left(e^{-(\overline{\overline{O_s}}(-\log(\overline{\overline{\alpha}}_{\overline{\overline{R_1}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{O_s}}(-\log(\overline{\overline{\alpha}}_{\overline{\overline{I_1}}}))^Z)^{1/Z}}\right)}, \\ 1 - \left(e^{-(\overline{\overline{O_s}}(-\log(1-\overline{\overline{\beta}}_{\overline{\overline{R_1}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{O_s}}(-\log(1-\overline{\overline{\beta}}_{\overline{\overline{I_1}}}))^Z)^{1/Z}}\right)}, \\ \left(1 - e^{-(\overline{\overline{O_s}}(-\log(1-\overline{\overline{\gamma}}_{\overline{\overline{R_1}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{O_s}}(-\log(1-\overline{\overline{\gamma}}_{\overline{\overline{I_1}}}))^Z)^{1/Z}}\right)}. \end{array} \right)$$

Definition 2.6. The currently used score and accuracy functions for any two CSV-NSs are listed below. The score function is $\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu 1}}})$ is calculated as:

$$\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_1}}}) = 1/3(\overline{\overline{\alpha_{R_1}}} + \overline{\overline{\alpha_{I_1}}} - \overline{\overline{\beta}}_{\overline{R_1}} - \overline{\overline{\beta}}_{\overline{I_I}} - \overline{\overline{\gamma}}_{\overline{R_1}} - \overline{\overline{\gamma}}_{\overline{R_2}}), \quad \overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_1}}}) \in [-1, 1]$$

Combining the degrees of truth, indeterminacy, and falsity in both real and imaginary sections of the CSV-NS helps this function to reflect the net confidence. Analogously, the accuracy function $\overline{\overline{Y_{AV}}}(\overline{\overline{\mu_1}})$ is defined as

$$\overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_1}}}) = 1/3(\overline{\overline{\alpha_{R_1}}} + \overline{\overline{\alpha_{I_1}}} + \overline{\overline{\beta}}_{\overline{R_1}} + \overline{\overline{\beta}}_{\overline{I_I}} + \overline{\overline{\gamma}}_{\overline{R_1}} + \overline{\overline{\gamma}}_{\overline{R_2}}), \quad \overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_1}}}) \in [0, 1]$$

This function calculates the overall information or completeness of a CSV-NS by combining all the related real and imaginary parts of truth, uncertainty, and falsehood.

Remark 2.7. The CSV-NSs exhibit several notable comparative features based on the score and accuracy functions, which are outlined as follows:

(1) If $\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_1}}}) > \overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_2}}})$, then $\overline{\overline{C_{\mu_1}}}$ is considered superior to $\overline{\overline{C_{\mu_2}}}$.
(2) If $\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_1}}}) < \overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_2}}})$, then $\overline{\overline{C_{\mu_1}}}$ is considered inferior to $\overline{\overline{C_{\mu_2}}}$.
(3) If $\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_1}}}) = \overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu_2}}})$, then the accuracy function is used for tie-breaking:
  (i) If $\overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_1}}}) > \overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_2}}})$, then $\overline{\overline{C_{\mu_1}}}$ is superior to $\overline{\overline{C_{\mu_2}}}$.
  (ii) If $\overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_1}}}) < \overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_2}}})$, then $\overline{\overline{C_{\mu_1}}}$ is inferior to $\overline{\overline{C_{\mu_2}}}$.
  (iii) If $\overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_1}}}) = \overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu_2}}})$, then $\overline{\overline{C_{\mu_1}}}$ and $\overline{\overline{C_{\mu_2}}}$ are considered equivalent.

Example 2.8. Building on Example 3.4 (Network intrusion detection), examine two assault patterns shown as CSV-NSs:

$$\overline{\overline{C_{\mu 1}}} = (0.8e^{i2\pi(0.7)}, 0.3e^{i2\pi(0.2)}, 0.4e^{i2\pi(0.1)})$$
$$\overline{\overline{C_{\mu 2}}} = (0.7e^{i2\pi(0.6)}, 0.2e^{i2\pi(0.3)}, 0.5e^{i2\pi(0.2)})$$

Calculate their values of accuracy and score:

$$\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu 1}}}) = \frac{1}{3}(0.8 + 0.7 - 0.3 - 0.2 - 0.4 - 0.1) = 0.16$$
$$\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu 2}}}) = \frac{1}{3}(0.7 + 0.6 - 0.2 - 0.3 - 0.5 - 0.2) = 0.03$$
$$\overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu 1}}}) = \frac{1}{3}(0.8 + 0.7 + 0.3 + 0.2 + 0.4 + 0.1) = 0.84$$
$$\overline{\overline{Y_{AV}}}(\overline{\overline{C_{\mu 2}}}) = \frac{1}{3}(0.7 + 0.6 + 0.2 + 0.3 + 0.5 + 0.2) = 0.83$$

By the ranking rules:

- $\overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu 1}}}) > \overline{\overline{Y_{SV}}}(\overline{\overline{C_{\mu 2}}}) \Rightarrow \overline{\overline{C_{\mu 1}}}$ is more severe
- The higher accuracy of $\overline{\overline{C_{\mu 1}}}$ confirms its reliability

Proposition 2.9 (Monotonicity of CSV-NS measures)**.** *The score and accuracy functions of any CSV-NS* ($\overline{\overline{C_\mu}}$) *fulfill:*

(1) $\overline{\overline{Y_{SV}}}(\overline{\overline{C_\mu}})$ *is strictly decreasing in* $\overline{\overline{\beta}}_{\overline{\overline{R}}}$, $\overline{\overline{\beta}}_{\overline{\overline{I}}}$, $\overline{\overline{\gamma}}_{\overline{\overline{R}}}$, *and* $\overline{\overline{\gamma}}_{\overline{\overline{I}}}$

(2) $\overline{\overline{Y_{AV}}}(\overline{\overline{C_\mu}})$ *is strictly increasing in all components* $\overline{\overline{\alpha}}_{\overline{\overline{R}}}$, $\overline{\overline{\alpha}}_{\overline{\overline{I}}}$, $\overline{\overline{\beta}}_{\overline{\overline{R}}}$, $\overline{\overline{\beta}}_{\overline{\overline{I}}}$, $\overline{\overline{\gamma}}_{\overline{\overline{R}}}$, *and* $\overline{\overline{\gamma}}_{\overline{\overline{I}}}$

Corollary 2.10 (Boundary cases)**.** *For extremes of CSV-NS values:*

- *When* $\overline{\overline{\alpha}}_{\overline{\overline{R}}} = \overline{\overline{\alpha}}_{\overline{\overline{I}}} = 1$ *and all others zero:* $\overline{\overline{Y_{SV}}} = \frac{2}{3}$, $\overline{\overline{Y_{AV}}} = \frac{2}{3}$
- *When* $\overline{\overline{\gamma}}_{\overline{\overline{R}}} = \overline{\overline{\gamma}}_{\overline{\overline{I}}} = 1$ *and all others zero:* $\overline{\overline{Y_{SV}}} = -\frac{2}{3}$, $\overline{\overline{Y_{AV}}} = \frac{2}{3}$
- *The neutral case* $\overline{\overline{R}} = 1e^{i2\pi(1)}$ *yields:* $\overline{\overline{Y_{SV}}} = 0$, $\overline{\overline{Y_{AV}}} = 0$

Theorem 2.11. *The next qualities and algebraic features remain true for every pair of CSV-NSs:*

(1) $\overline{\overline{C_{\overline{\overline{\mu_1}}}}} \oplus \overline{\overline{C_{\overline{\overline{\mu_2}}}}} = \overline{\overline{C_{\overline{\overline{\mu_2}}}}} \oplus \overline{\overline{C_{\overline{\overline{\mu_1}}}}}$;

(2) $\overline{\overline{C_{\overline{\overline{\mu_1}}}}} \otimes \overline{\overline{C_{\overline{\overline{\mu_2}}}}} = \overline{\overline{C_{\overline{\overline{\mu_2}}}}} \otimes \overline{\overline{C_{\overline{\overline{\mu_1}}}}}$;

(3) $\overline{\overline{O_s}}\left(\overline{\overline{C_{\overline{\overline{\mu_1}}}}} \oplus \overline{\overline{C_{\overline{\overline{\mu_2}}}}}\right) = \overline{\overline{O_s C_{\mu_1}}} \oplus \overline{\overline{O_s C_{\mu_2}}}$;

(4) $\left(\overline{\overline{O_{s_1}}} + \overline{\overline{O_{s_2}}}\right)\overline{\overline{C_{\mu_1}}} = \overline{\overline{O_{s_1} C_{\mu_1}}} \oplus \overline{\overline{O_{s_2} C_{\mu_1}}}$;

(5) $\left(\overline{\overline{C_{\mu_1}}} \otimes \overline{\overline{C_{\mu_2}}}\right)^{\overline{\overline{O_s}}} = \overline{\overline{C_{\mu_1}}}^{\overline{\overline{O_s}}} \otimes \overline{\overline{C_{\mu_2}}}^{\overline{\overline{O_s}}}$;

(6) $\overline{\overline{C_{\mu_1}}}^{\overline{\overline{O_{s_1}}}} \otimes \overline{\overline{C_{\mu_1}}}^{\overline{\overline{O_{s_2}}}} = \overline{\overline{C_{\mu_1}}}^{\overline{\overline{O_{s_1}}}+\overline{\overline{O_{s_2}}}}$.

3. The Proposed Aczel-Alsina Power AOs for CSV-NSs

Here, we offer various power AOs designed using A-A rules to successfully supervise and handle CSV-NSs. We recognize four types of operators: the CSV-NSs CPF-AAP-A, the CSV-NSs CPF-AAWP-A, the CSV-NSs CPF-AAP-G, and the CSV-NSs CPF-AAWP-G. Such tools are intended for working with CSV-NS and decision situations, and their important traits are explored in the following parts of this chapter. Since these data operators handle unclear or complex data well, they are helpful in programs that deal with computer-based algorithms for learning.

3.1. *CSV-NS Aczel-Alsina Power Aggregation Operators*

Here, we propose the aggregation operators:

Definition 3.1. Let $\{\overline{C}_{\mu_I}\}_{I=1}^{l}$ be a collection of CSV-NSs where each $\overline{C}_{\mu_I} = \langle T_I, I_I, F_I\rangle$ with:

$$T_I = p_I e^{i2\pi\omega_I} \quad \text{(Truth membership)}$$

$$I_I = q_I e^{i2\pi\psi_I} \quad \text{(Indeterminacy membership)}$$

$$F_I = r_I e^{i2\pi\phi_I} \quad \text{(Falsehood membership)}$$

(1) **CSV-NS Aczel-Alsina Power Average (CSV-AAP-A) Operator**:

$$\text{CSV-AAP-A}(\overline{C}_{\mu_1}, \ldots, \overline{C}_{\mu_l}) = \bigoplus_{I=1}^{l} \left(\Psi_I \overline{C}_{\mu_I}\right) \tag{1}$$

(2) **CSV-NS Aczel-Alsina Weighted Power Average (CSV-AAWP-A) Operator**:

$$\text{CSV-AAWP-A}(\overline{C}_{\mu_1}, \ldots, \overline{C}_{\mu_l}) = \bigoplus_{I=1}^{l} \left(w_I \Psi_I \overline{C}_{\mu_I}\right) \tag{2}$$

where:

- Weight coefficients Ψ_I are determined by:

$$\Psi_I = \frac{1 + V(\overline{C}_{\mu_I})}{\sum_{I=1}^{l}(1 + V(\overline{C}_{\mu_I}))} \tag{3}$$

- Support measure $V(\overline{C}_{\mu_I})$ captures interrelationships:

$$V(\overline{C}_{\mu_I}) = \sum_{\substack{s=1 \\ s \neq I}}^{l} \text{Sup}(\overline{C}_{\mu_I}, \overline{C}_{\mu_s})$$

- Support function based on distance:

$$\text{Sup}(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) = 1 - d(\overline{C}_{\mu_I}, \overline{C}_{\mu_s})$$

- Comprehensive CSV-NS distance metric:

$$\begin{aligned} d(\overline{C}_{\mu_I}, \overline{C}_{\mu_s}) = \frac{1}{6}\Big[&|p_I - p_s| + |\omega_I - \omega_s| \\ &+ |q_I - q_s| + |\psi_I - \psi_s| \\ &+ |r_I - r_s| + |\phi_I - \phi_s|\Big] \end{aligned}$$

These operators extend the Aczel-Alsina power aggregation framework specifically for CSV-NSs, maintaining:

- Closure property under CSV-NS operations
- Magnitude-phase consistency in complex domain
- Boundary conditions: $0 \leq p_I + q_I + r_I \leq 3$
- Phase periodicity: $\omega_I, \psi_I, \phi_I \in [0, 1]$

Theorem 3.2. *We show that the resulting formulation is really derived from the CSV-NSs model in line with Eqs. 4 and 5 and may be stated as:*

$$
\begin{aligned}
&CPF\text{-}AAP\text{-}A(\overline{\overline{C_{\mu_1}}}, \overline{\overline{C_{\mu_2}}}, \ldots, \overline{\overline{C_{\mu_l}}}) \\
&= \left(\begin{array}{c}
\left(1 - e^{-\left(\sum\limits_{I=1}^{l} \overline{\overline{\Psi_I}}\left(-\log(1-\overline{\overline{\alpha_{\overline{\overline{R_I}}}}})\right)^Z\right)^{1/Z}}\right) e^{i2\pi\left(1-e^{-\left(\sum\limits_{I=1}^{l} \overline{\overline{\Psi_I}}\left(-\log(1-\overline{\overline{\alpha_{\overline{\overline{I_I}}}}})\right)^Z\right)^{1/Z}}\right)}, \\
\left(e^{-\left(\sum\limits_{I=1}^{l} \overline{\overline{\Psi_I}}\left(-\log(1-\overline{\overline{\beta_{\overline{\overline{R_I}}}}})\right)^Z\right)^{1/Z}}\right) e^{i2\pi\left(e^{-\left(\sum\limits_{I=1}^{l} \overline{\overline{\Psi_I}}\left(-\log(1-\overline{\overline{\beta_{\overline{\overline{I_I}}}}})\right)^Z\right)^{1/Z}}\right)}, \\
\left(e^{-\left(\sum\limits_{I=1}^{l} \overline{\overline{\Psi_I}}\left(-\log(1-\overline{\overline{\gamma_{\overline{\overline{R_I}}}}})\right)^Z\right)^{1/Z}}\right) e^{i2\pi\left(e^{-\left(\sum\limits_{I=1}^{l} \overline{\overline{\Psi_I}}\left(-\log(1-\overline{\overline{\gamma_{\overline{\overline{I_I}}}}})\right)^Z\right)^{1/Z}}\right)}.
\end{array} \right)
\end{aligned}
$$

Proof. We then work using induction in mathematics. The base case $l = 2$ results in

$$
\overline{\overline{\Psi_1 C_{\mu 1}}} = \left(\begin{array}{c}
\left(1 - e^{-(\overline{\overline{\Psi_1}}(-\log(1-\overline{\overline{\alpha_{\overline{\overline{R_1}}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(1-\overline{\overline{\alpha_{\overline{\overline{I_1}}}}}))^Z)^{1/Z}}\right)}, \\
\left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\beta_{\overline{\overline{R_1}}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\beta_{\overline{\overline{I_1}}}}}))^Z)^{1/Z}}\right)}, \\
\left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{\overline{R_1}}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{\overline{I_1}}}}}))^Z)^{1/Z}}\right)}.
\end{array} \right)
$$

$$
\overline{\overline{\Psi_1 C_{\mu 1}}} = \left(\begin{array}{c}
\left(1 - e^{-(\overline{\overline{\Psi_1}}(-\log(1-\overline{\overline{\alpha_{\overline{\overline{R_1}}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(1-\overline{\overline{\alpha_{\overline{\overline{I_1}}}}}))^Z)^{1/Z}}\right)}, \\
\left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\beta_{\overline{\overline{R_1}}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\beta_{\overline{\overline{I_1}}}}}))^Z)^{1/Z}}\right)}, \\
\left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{\overline{R_1}}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{\overline{I_1}}}}}))^Z)^{1/Z}}\right)}.
\end{array} \right)
$$

$$\overline{\overline{\Psi_2 C_{\mu 2}}} = \left(\begin{array}{c} \left(1 - e^{-(\overline{\overline{\Psi_2}}(-\log(1-\overline{\overline{\alpha_{\overline{R_2}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_2}}(-\log(1-\overline{\overline{\alpha_{\overline{I_2}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\beta_{\overline{R_2}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\beta_{\overline{I_2}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\gamma_{\overline{R_2}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\gamma_{\overline{I_2}}}}))^Z)^{1/Z}}\right)}. \end{array} \right)$$

Thus,

$$\begin{aligned} \text{CPF-AAP-A}(\overline{\overline{C_{\mu_1}}}, \overline{\overline{C_{\mu_2}}}) &= \overline{\overline{\Psi_1 C_{\mu 1}}} \oplus \overline{\overline{\Psi_2 C_{\mu 2}}} \\ &= \left(\begin{array}{c} \left(1 - e^{-(\overline{\overline{\Psi_1}}(-\log(1-\overline{\overline{\alpha_{\overline{R_1}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_1}}(-\log(1-\overline{\overline{\alpha_{\overline{I_1}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\beta_{\overline{R_1}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\beta_{\overline{I_1}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{R_1}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{I_1}}}}))^Z)^{1/Z}}\right)}, \end{array} \right) \\ &\oplus \left(\begin{array}{c} \left(1 - e^{-(\overline{\overline{\Psi_2}}(-\log(1-\overline{\overline{\alpha_{\overline{R_2}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_2}}(-\log(1-\overline{\overline{\alpha_{\overline{I_2}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\beta_{\overline{R_2}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\beta_{\overline{I_2}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_1}}(-\log(\overline{\overline{\gamma_{\overline{R_2}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{\Psi_2}}(-\log(\overline{\overline{\gamma_{\overline{I_2}}}}))^Z)^{1/Z}}\right)}. \end{array} \right) \\ &= \left(\begin{array}{c} \left(1 - e^{-(\sum_{I=1}^{2} \overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{\overline{R_I}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\sum_{I=1}^{2} \overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{\overline{I_I}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{2} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\alpha_{\overline{R_I}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{2} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\alpha_{\overline{I_I}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{2} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{\overline{R_I}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{2} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{\overline{I_I}}}}))^Z)^{1/Z}}\right)}. \end{array} \right) \end{aligned}$$

We are correct. We also hold the statement in the case where $l = k$. We then deal with.

$$\text{CPF-AAP-A}(\overline{\overline{C_{\mu_1}}}, \overline{\overline{C_{\mu_2}}}, ..., \overline{\overline{C_{\mu_l}}})$$

$$= \begin{pmatrix} \left(1 - e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{I_I}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\beta_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi e\left(-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\beta_{I_I}}}))^Z)^{1/Z}\right)}, \\ \left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{I_I}}}))^Z)^{1/Z}}\right)}. \end{pmatrix}$$

So for $k + 1 = 1$,we get

$$\text{CPF-AAP-A}(\overline{\overline{C_{\mu_1}}}, \overline{\overline{C_{\mu_2}}}, ..., \overline{\overline{C_{\mu_l}}}) = \oplus_{I=1}^{k+1}(\overline{\overline{\Psi_I C_{\mu_I}}}) = \oplus_{I=1}^{k}(\overline{\overline{\Psi_I C_{\mu_I}}}) \oplus \overline{\overline{\Psi_{k+1} C_{\mu_{k+1}}}}$$

$$= \begin{pmatrix} \left(1 - e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{I_I}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\beta_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\beta_{I_I}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{k} \overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{I_I}}}))^Z)^{1/Z}}\right)}, \end{pmatrix}$$

$$\oplus \begin{pmatrix} \left(1 - e^{-(\overline{\overline{\Psi_{k+1}}}(-\log(1-\overline{\overline{\alpha_{R_{k+1}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\overline{\overline{\Psi_{k+1}}}(-\log(1-\overline{\overline{\alpha_{I_{k+1}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_{k+1}}}(-\log(\overline{\overline{\beta_{R_{k+1}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{\Psi_{k+1}}}(-\log(\overline{\overline{\beta_{I_{k+1}}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\overline{\overline{\Psi_{k+1}}}(-\log(\overline{\overline{\gamma_{R_{k+1}}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\overline{\overline{\Psi_{k+}}}(-\log(\overline{\overline{\gamma_{I_{k+1}}}}))^Z)^{1/Z}}\right)}. \end{pmatrix}$$

$$= \left(\begin{array}{c} \left(1-e^{-(\sum_{I=1}^{k+1}\overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-(\sum_{I=1}^{k+1}\overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{I_I}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{k+1}\overline{\overline{\Psi_I}}(-\log(\overline{\overline{\beta_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{k+1}\overline{\overline{\Psi_I}}(-\log(\overline{\overline{\beta_{I_I}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-(\sum_{I=1}^{k+1}\overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{R_I}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-(\sum_{I=1}^{k+1}\overline{\overline{\Psi_I}}(-\log(\overline{\overline{\gamma_{I_I}}}))^Z)^{1/Z}}\right)}. \end{array} \right)$$

□

Proposition 3.3. ***(Idempotency)***. *Taking it that all good things about the company are factual, if* $\overline{\overline{C_{\mu I}}} = \overline{\overline{C}}$ *for all* I*, then*

$$CPF\text{-}AAP\text{-}A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{C}}.$$

Proof. Notice that we have

$$\overline{\overline{C_{\mu I}}} = \overline{\overline{C}} = (\overline{\overline{\alpha_R}}e^{i2\pi(\overline{\overline{\alpha_I}})}, \overline{\overline{\beta_R}}e^{i2\pi(\overline{\overline{\beta_I}})}, \overline{\overline{\gamma_R}}e^{i2\pi(\overline{\overline{\gamma_I}})}).$$

Then

$$\begin{aligned} &\text{CPF-AAP-A}(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, ..., \overline{\overline{C_{\mu l}}}) \\ &= \left(\begin{array}{c} \left(1-e^{-(\sum_{I-1}^{l}\overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{R_I}}}))Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-((\sum_{I-1}^{l}\overline{\overline{\Psi_I}}(-\log(1-\overline{\overline{\alpha_{R_I}}}))^Z)^{1/Z}}\right)}, \\ \left(e^{-\sum_{I=1}^{l}\overline{\overline{\Psi}}_I(-\log(\overline{\overline{\beta_{R_I}}}))^{Z)^{1/Z}}}\right) e^{i2\pi\left((e\left(^{-\sum_{I=1}^{l}\overline{\overline{\Psi}}_I(-\log(\overline{\overline{\beta_{R_I}}}))^Z)^{1/Z}}\right)\right)}, \\ \left(e^{-\sum_{I=1}^{l}\overline{\overline{\Psi}}_I(-\log(\overline{\overline{\gamma_{R_I}}}))^{Z)^{1/Z}}}\right) e^{i2\pi(e^{-\sum_{I=1}^{l}\overline{\overline{\Psi}}_I(-\log(\overline{\overline{\gamma_{R_I}}}))^Z)^{1/Z}})}. \end{array} \right) \\ &= \left(\begin{array}{c} \left(1-e^{-((-\log(1-\overline{\overline{\alpha_{RI}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(1-e^{-((-\log(1-\overline{\overline{\alpha_I}}))^Z)1Z}\right)}, \\ \left(\left(e^{-((-\log(-\overline{\overline{\beta_{RI}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-((-\log(-\overline{\overline{\beta_{RI}}}))^Z)^{1/Z}}\right)}, \right. \\ \left.\left(\left(e^{-((-\log(-\overline{\overline{\gamma_{RI}}}))^Z)^{1/Z}}\right) e^{i2\pi\left(e^{-((-\log(-\overline{\overline{\gamma_{RI}}}))^Z)^{1/Z}}\right)}\right). \end{array} \right) \\ &= \left(\left(1-e^{\log(1-\overline{\overline{\alpha_R}})}\right) e^{i2\pi(1-e^{\log(1-\overline{\overline{\alpha_I}})}}, \left(e^{\log(\overline{\overline{\beta_R}})}\right) e^{i2\pi(e^{\log(\overline{\overline{\beta_I}})}}, \left(e^{\log(\overline{\overline{\gamma_R}})}\right) e^{i2\pi(e^{\log(\overline{\overline{\gamma_I}})}}\right). \end{aligned}$$

$$= \left(\overline{\overline{\alpha_R}} e^{i2\pi(\overline{\overline{\alpha_I}})}, \overline{\overline{\beta_R}} e^{i2\pi(\overline{\overline{\beta_I}})}, \overline{\overline{\gamma_R}} e^{i2\pi(\overline{\overline{\gamma_I}})} \right).$$

Next, we are concerned with whether the

$$CPF - AAP - A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, ..., \overline{\overline{C_{\mu l}}}),$$

satisfies the monotonicity constraint. In other words, the assertion"If

$$\overline{\overline{C_{\mu I}}} \leq \overline{\overline{C_{\mu I}}}' = (\overline{\overline{\alpha_{R_I}}}' e^{i2\pi(\overline{\overline{\alpha_{I_I}}}')}, \overline{\overline{\beta_{R_I}}}' e^{i2\pi(\overline{\overline{\beta_{I_I}}}')}, \overline{\overline{\gamma_{R_I}}}' e^{i2\pi(\overline{\overline{\gamma_{I_I}}}')},$$

then

$$CPF - AAP - A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, ..., \overline{\overline{C_{\mu l}}}) \leq CPF - AAP - A(\overline{\overline{C_{\mu 1}}}', \overline{\overline{C_{\mu 2}}}', ..., \overline{\overline{C_{\mu l}}}')$$

is accurate or not". In response, we say that our claim is false, which means that "if

$$\overline{\overline{C_{\mu I}}} \leq \overline{\overline{C_{\mu I}}}',$$

then

$$CPF - AAP - A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, ..., \overline{\overline{C_{\mu l}}}) \not\leq CPF - AAP - A(\overline{\overline{C_{\mu 1}}}', \overline{\overline{C_{\mu 2}}}', ..., \overline{\overline{C_{\mu l}}}')"$$

□

Example 3.4. It is important for a cybersecurity system to watch for network activity and place anything it observes in the categories of a *safe connection*, *DDoS attack*, or *malware intrusion*. The features used are CSV-NS for the purposes of classification.

Table 1. CSV-NS Representations for Three Events

Event	$\overline{\overline{\alpha}}$	$\overline{\overline{\beta}}$	$\overline{\overline{\gamma}}$
$\overline{\overline{C_{\mu 1}}}$	$0.8e^{i2\pi(0.3)}$	$0.1e^{i2\pi(0.2)}$	$0.2e^{i2\pi(0.1)}$
$\overline{\overline{C_{\mu 2}}}$	$0.6e^{i2\pi(0.4)}$	$0.3e^{i2\pi(0.1)}$	$0.1e^{i2\pi(0.2)}$
$\overline{\overline{C_{\mu 3}}}$	$0.7e^{i2\pi(0.2)}$	$0.2e^{i2\pi(0.3)}$	$0.3e^{i2\pi(0.0)}$

Solution The CPF-AAP-A aggregation with weights $\overline{\overline{\Psi_1}} = 0.337$, $\overline{\overline{\Psi_2}} = 0.320$, $\overline{\overline{\Psi_3}} = 0.343$ yields:

Falsity-Membership ($\overline{\overline{\beta}}$) Aggregation

$$\begin{aligned}
\overline{\overline{\beta_{\text{agg}}}} &= \bigoplus_{k=1}^{3} \overline{\overline{\Psi_k}} \cdot \overline{\overline{\beta_k}} \\
&= 0.337 \cdot 0.1e^{i2\pi(0.2)} + 0.320 \cdot 0.3e^{i2\pi(0.1)} + 0.343 \cdot 0.2e^{i2\pi(0.3)} \\
&= 0.337 \cdot (0.1\cos(0.4\pi) + i0.1\sin(0.4\pi)) \\
&\quad + 0.320 \cdot (0.3\cos(0.2\pi) + i0.3\sin(0.2\pi)) \\
&\quad + 0.343 \cdot (0.2\cos(0.6\pi) + i0.2\sin(0.6\pi)) \\
&\approx (0.0259 + i0.0198) + (0.0888 + i0.0309) + (0.0343 - i0.0594) \\
&= (0.1490 - i0.0087) \\
\|\overline{\overline{\beta_{\text{agg}}}}\| &= \sqrt{(0.1490)^2 + (-0.0087)^2} \approx 0.149
\end{aligned}$$

Indeterminacy-Membership ($\overline{\overline{\gamma}}$) Aggregation

$$\begin{aligned}
\overline{\overline{\gamma_{\text{agg}}}} &= \bigoplus_{k=1}^{3} \overline{\overline{\Psi_k}} \cdot \overline{\overline{\gamma_k}} \\
&= 0.337 \cdot 0.2e^{i2\pi(0.1)} + 0.320 \cdot 0.1e^{i2\pi(0.2)} + 0.343 \cdot 0.3e^{i2\pi(0.0)} \\
&= 0.337 \cdot (0.2\cos(0.2\pi) + i0.2\sin(0.2\pi)) \\
&\quad + 0.320 \cdot (0.1\cos(0.4\pi) + i0.1\sin(0.4\pi)) \\
&\quad + 0.343 \cdot (0.3\cos(0) + i0.3\sin(0)) \\
&\approx (0.0539 + i0.0198) + (0.0247 + i0.0187) + (0.1029 + i0) \\
&= (0.1815 + i0.0385) \\
\|\overline{\overline{\gamma_{\text{agg}}}}\| &= \sqrt{(0.1815)^2 + (0.0385)^2} \approx 0.185
\end{aligned}$$

The truth-membership aggregation yields:

$$\|\overline{\overline{\alpha_{\text{agg}}}}\| \approx 0.7$$

Final decision on classification:

$$\|\overline{\overline{\alpha_{\text{agg}}}}\| = 0.7 > \|\overline{\overline{\beta_{\text{agg}}}}\| = 0.149 \quad \text{and} \quad \|\overline{\overline{\gamma_{\text{agg}}}}\| = 0.185$$

For this reason, the system has classified it as an **attack**. CSV-NS gives users three main benefits:

(1) *Uncertainty handling*: Using complex exponents, we are able to model the periodic changes found in encrypted traffic.

(2) *Dynamic weighting*: Similarity-based weights change as events are correlated differently.

(3) *ML integration*: Neural networks and fuzzy systems are compatible with the system.

Definition 3.5. The computational notation for CPF-AAWP-A operator is

$$CPF\text{-}AAP\text{-}A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{\Psi_1 C_{\mu 1}}} \oplus \overline{\overline{\Psi_2 C_{\mu 2}}} \oplus \cdots \oplus \overline{\overline{\Psi_l C_{\mu l}}} = \bigoplus_{I=1}^{l} \left(\overline{\overline{\Psi_I C_{\mu I}}} \right) \quad (4)$$

$$\overline{\overline{\Psi_I}} = WPA(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \frac{\Phi_I(1 + V(\overline{\overline{C_{\mu I}}}))}{\sum_{I=1}^{l} \Phi_I(1 + V(\overline{\overline{C_{\mu I}}}))} \quad (5)$$

Note that the weight vector $\Phi_I \in [0,1]$ satisfies $\sum_{I=1}^{l} \Phi_I = 1$.

Theorem 3.6. *From Eqs. 4 and 5, we clearly see that the above theory is again represented by CSV-NSs.*

$$CPF\text{-}AAWP\text{-}A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}})$$

$$= \left(\begin{array}{c} \left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log(1-\overline{\overline{\alpha_{R_I}}})\right)^Z\right)^{\frac{1}{Z}}}\right) e^{i2\pi\left(1-e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log(1-\overline{\overline{\alpha_{I_I}}})\right)^U\right)^{\frac{1}{U}}}\right)}, \\ \left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log(\overline{\overline{\beta_{R_I}}})\right)^Z\right)^{\frac{1}{Z}}}\right) e^{i2\pi\left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log(\overline{\overline{\beta_{I_I}}})\right)^Z\right)^{\frac{1}{Z}}}\right)}, \\ \left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{K_I}} \left(-\log(\overline{\overline{\gamma_{R_I}}})\right)^Z\right)^{\frac{1}{Z}}}\right) e^{i2\pi\left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{K_I}} \left(-\log(\overline{\overline{\gamma_{I_I}}})\right)^Z\right)^{\frac{1}{Z}}}\right)} \end{array} \right)$$

Proof. The proof using mathematical induction resembles that of Theorem 3.2. □

Proposition 3.7. ***(Idempotency)*** *Should all combined inputs be exact, i.e., $\overline{\overline{C_{\mu I}}} = \overline{\overline{C}}$ for all I, The CPF-AAWP-A operator then outputs the same: $CPF\text{-}AAWP\text{-}A(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{C}}$.*

Proof. The evidence is like that of Proposition 3.3. □

Example 3.8. Three network traffic events $\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \overline{\overline{C_{\mu 3}}}$analysis by an AI system with intricate CSV-NSs. The membership degrees show themselves as exponential shape as follows:

Solution With weights $\Phi = (0.25, 0.45, 0.30)$ and support measures, the CPF-AAWP-A operator shows:

$$V(\overline{\overline{C_{\mu 1}}}) = 1.75, \quad V(\overline{\overline{C_{\mu 2}}}) = 1.76, \quad V(\overline{\overline{C_{\mu 3}}}) = 1.71$$

Table 2. CSV-NS Parameters in Exponential Form

Event	$\overline{\overline{\alpha}}$	$\overline{\overline{\beta}}$	$\overline{\overline{\gamma}}$
$\overline{\overline{C_{\mu 1}}}$	$0.865e^{i2\pi(0.15)}$	$0.112e^{i2\pi(0.40)}$	$0.291e^{i2\pi(0.14)}$
$\overline{\overline{C_{\mu 2}}}$	$0.790e^{i2\pi(0.25)}$	$0.212e^{i2\pi(0.30)}$	$0.290e^{i2\pi(0.15)}$
$\overline{\overline{C_{\mu 3}}}$	$0.829e^{i2\pi(0.12)}$	$0.262e^{i2\pi(0.48)}$	$0.206e^{i2\pi(0.05)}$

We calculate priorities using weights

$$\overline{\overline{\Psi_1}} = \frac{0.25(1+1.75)}{0.25(2.75)+0.45(2.76)+0.30(2.68)} = 0.252$$
$$\overline{\overline{\Psi_2}} = \frac{0.45(1+1.76)}{\text{Denominator}} = 0.455$$
$$\overline{\overline{\Psi_3}} = \frac{0.30(1+1.71)}{\text{Denominator}} = 0.293$$

Falsity-Membership ($\overline{\overline{\beta}}$) Aggregation

$$\begin{aligned}
\overline{\overline{\beta_{\text{agg}}}} &= \bigoplus_{k=1}^{3} \overline{\overline{\Psi_k}} \cdot \overline{\overline{\beta_k}} \\
&= 0.252 \cdot 0.112e^{i2\pi(0.40)} + 0.455 \cdot 0.212e^{i2\pi(0.30)} + 0.293 \cdot 0.262e^{i2\pi(0.48)} \\
&= 0.252 \cdot (0.112\cos(0.8\pi) + i0.112\sin(0.8\pi)) \\
&\quad + 0.455 \cdot (0.212\cos(0.6\pi) + i0.212\sin(0.6\pi)) \\
&\quad + 0.293 \cdot (0.262\cos(0.96\pi) + i0.262\sin(0.96\pi)) \\
&\approx (0.0282 - i0.0217) + (0.0459 + i0.0789) + (-0.0765 + i0.0258) \\
&= (-0.0024 + i0.0830) \\
\|\overline{\overline{\beta_{\text{agg}}}}\| &= \sqrt{(-0.0024)^2 + (0.0830)^2} \approx 0.083
\end{aligned}$$

Indeterminacy-Membership ($\overline{\overline{\gamma}}$) Aggregation

$$
\begin{aligned}
\overline{\overline{\gamma_{\text{agg}}}} &= \bigoplus_{k=1}^{3} \overline{\overline{\Psi}_k} \cdot \overline{\overline{\gamma_k}} \\
&= 0.252 \cdot 0.291 e^{i2\pi(0.14)} + 0.455 \cdot 0.290 e^{i2\pi(0.15)} + 0.293 \cdot 0.206 e^{i2\pi(0.05)} \\
&= 0.252 \cdot (0.291 \cos(0.28\pi) + i0.291 \sin(0.28\pi)) \\
&\quad + 0.455 \cdot (0.290 \cos(0.30\pi) + i0.290 \sin(0.30\pi)) \\
&\quad + 0.293 \cdot (0.206 \cos(0.10\pi) + i0.206 \sin(0.10\pi)) \\
&\approx (0.0689 + i0.0251) + (0.1129 + i0.0449) + (0.0589 + i0.0095) \\
&= (0.2407 + i0.0795) \\
\|\overline{\overline{\gamma_{\text{agg}}}}\| &= \sqrt{(0.2407)^2 + (0.0795)^2} \approx 0.253
\end{aligned}
$$

Results of final evaluation reveal:

$$\|\overline{\overline{\alpha_{\text{agg}}}}\| = 0.793 > \|\overline{\overline{\beta_{\text{agg}}}}\| = 0.083 \quad \text{and} \quad \|\overline{\overline{\gamma_{\text{agg}}}}\| = 0.253$$

highly confident in verifying malware detection.

3.2. *Complex Single-Valued Neutrosophic Sets CPF-AAP-G and CPF-AAWP-G Operators*

As a solution to monotonicity, we introduce the CPF-AAP-G and CPF-AAWP-G operators, which we will describe in the following part of this Subsection 3.2.

Definition 3.9. We now define what the CPF-AAP-G operator means in a computational sense:

$$CPF\text{-}AAP\text{-}G(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{C_{\mu 1}}}^{\overline{\overline{\Psi_1}}} \otimes \overline{\overline{C_{\mu 2}}}^{\overline{\overline{\Psi_2}}} \otimes \cdots \otimes \overline{\overline{C_{\mu l}}}^{\overline{\overline{\Psi_l}}} = \otimes_{I=1}^{l} \left(\overline{\overline{C_{\mu I}}}^{\overline{\overline{\Psi_I}}} \right) \tag{6}$$

where the $\overline{\overline{\Psi_I}}$weights are derived from

$$\overline{\overline{\Psi_I}} = PA(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \frac{(1 + V(\overline{\overline{C_{\mu I}}}))\Phi_I}{\sum_{I=1}^{l}(1 + V(\overline{\overline{C_{\mu I}}}))\Phi_I} \tag{7}$$

representing the initial weight vector, Φ_I.

Theorem 3.10. *Using Eqs. 6 and 7, the CPF-AAP-G operators aggregation results can be expressed as shown in a CSV-NSs.*

$$
\begin{aligned}
&CPF\text{-}AAP\text{-}G(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) \\
&= \left(\begin{array}{c}
\left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(\overline{\overline{\alpha_{\overline{\overline{R_I}}}}}\right)\right)^U\right)^{\frac{1}{U}}} \right) e^{i2\pi\left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(\overline{\overline{\alpha_{\overline{\overline{I_I}}}}}\right)\right)^U\right)^{\frac{1}{U}}}\right)}, \\
\left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1-\overline{\overline{\beta_{\overline{\overline{R_I}}}}}\right)\right)^U\right)^{\frac{1}{U}}} \right) e^{i2\pi\left(1-e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1-\overline{\overline{\beta_{\overline{\overline{I_I}}}}}\right)\right)^U\right)^{\frac{1}{U}}}\right)}, \\
\left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1-\overline{\overline{\gamma_{\overline{\overline{R_I}}}}}\right)\right)^U\right)^{\frac{1}{U}}} \right) e^{i2\pi\left(1-e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1-\overline{\overline{\gamma_{\overline{\overline{I_I}}}}}\right)\right)^U\right)^{\frac{1}{U}}}\right)}.
\end{array} \right)
\end{aligned}
$$

Proof. Mathematical induction provides the evidence; it is similar to the proof of Theorem 3.6. □

Proposition 3.11. *(Idempotency) If all input values are equal (e.g., $\overline{\overline{C_{\mu I}}} = \overline{\overline{C}}$), the CPF-AAP-G operator will preserve this value during aggregation. $CPF\text{-}AAP\text{-}G(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{C}}$. This attribute ensures that the aggregate process remains consistent when the inputs are uniform.*

Proof. The proof is similar to that for the related idempotency property in Proposition 3.3. □

Example 3.12. Consider these three cryptographic protocol assessments. $\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \overline{\overline{C_{\mu 3}}}$ for privacy-preserving communication, defined as

TABLE 3. CSV-NS Parameters for Protocol Evaluations (exponential form)

Protocol	$\overline{\overline{\alpha}}$	$\overline{\overline{\beta}}$	$\overline{\overline{\gamma}}$
$\overline{\overline{C_{\mu 1}}}$	$0.94e^{i2\pi(0.03)}$	$0.10e^{i2\pi(0.18)}$	$0.24e^{i2\pi(0.15)}$
$\overline{\overline{C_{\mu 2}}}$	$0.81e^{i2\pi(0.035)}$	$0.19e^{i2\pi(0.12)}$	$0.26e^{i2\pi(0.09)}$
$\overline{\overline{C_{\mu 3}}}$	$0.86e^{i2\pi(0.027)}$	$0.24e^{i2\pi(0.16)}$	$0.19e^{i2\pi(0.04)}$

Solution We use the CPF-AAP-G aggregation operator with initial weights $\Phi = (0.28, 0.42, 0.30)$ to derive support measures.

$$V(\overline{\overline{C_{\mu 1}}}) = 1.72, \quad V(\overline{\overline{C_{\mu 2}}}) = 1.65, \quad V(\overline{\overline{C_{\mu 3}}}) = 1.68,$$

and priority weights:

$$\begin{aligned}
\overline{\overline{\Psi_1}} &= \frac{(1+1.72)\times 0.28}{(2.72\times 0.28)+(2.65\times 0.42)+(2.68\times 0.30)} = 0.281\\
\overline{\overline{\Psi_2}} &= \frac{(1+1.65)\times 0.42}{\text{Denominator}} = 0.419\\
\overline{\overline{\Psi_3}} &= \frac{(1+1.68)\times 0.30}{\text{Denominator}} = 0.300
\end{aligned}$$

The falsity-membership $\overline{\overline{\beta}}$ is aggregated as:

$$\begin{aligned}
\overline{\overline{\beta_{\text{agg}}}} &= \bigotimes_{k=1}^{3} \left(\overline{\overline{\beta_k}}\right)^{\overline{\overline{\Psi_k}}}\\
&= \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}\,(-\ln(0.10))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.18))^{0.5}\right)^{1/0.5}\right)}\\
&\quad \otimes \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}\,(-\ln(0.19))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.12))^{0.5}\right)^{1/0.5}\right)}\\
&\quad \otimes \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}\,(-\ln(0.24))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.16))^{0.5}\right)^{1/0.5}\right)}\\
&\approx 0.162 e^{i2\pi(0.142)}
\end{aligned}$$

Indeterminacy membership $\overline{\overline{\gamma}}$ is aggregated as:

$$\begin{aligned}
\overline{\overline{\gamma_{\text{agg}}}} &= \bigotimes_{k=1}^{3} \left(\overline{\overline{\gamma_k}}\right)^{\overline{\overline{\Psi_k}}}\\
&= \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}\,(-\ln(0.24))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.15))^{0.5}\right)^{1/0.5}\right)}\\
&\quad \otimes \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}\,(-\ln(0.26))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.09))^{0.5}\right)^{1/0.5}\right)}\\
&\quad \otimes \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}\,(-\ln(0.19))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.04))^{0.5}\right)^{1/0.5}\right)}\\
&\approx 0.218 e^{i2\pi(0.088)}
\end{aligned}$$

Final evaluation shows:

$$\|\overline{\overline{\alpha_{\text{agg}}}}\| = 0.823 > \|\overline{\overline{\beta_{\text{agg}}}}\| = 0.162 \quad \text{and} \quad \|\overline{\overline{\gamma_{\text{agg}}}}\| = 0.218$$

verifying high protection of privacy.

Definition 3.13. The CPF-AAWP-G operator has the following defined computational form:

$$CPF\text{-}AAWP\text{-}G(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{C_{\mu 1}}}^{\overline{\overline{\Psi_1}}} \otimes \overline{\overline{C_{\mu 2}}}^{\overline{\overline{\Psi_2}}} \otimes \cdots \otimes \overline{\overline{C_{\mu l}}}^{\overline{\overline{\Psi_l}}} = \bigotimes_{I=1}^{l} \left(\overline{\overline{C_{\mu I}}}^{\overline{\overline{\Psi_I}}} \right) \tag{8}$$

where the weights $\overline{\overline{\Psi_I}}$ are calculated by the weighted prioritization aggregation (WPA) method as

$$\overline{\overline{\Psi_I}} = WPA(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \frac{\Phi_I(1 + V(\overline{\overline{C_{\mu l}}}))\overline{\overline{C_{\mu l}}}}{\sum_{I=1}^{l} \Phi_I(1 + V(\overline{\overline{C_{\mu l}}}))} \tag{9}$$

Theorem 3.14. *Examining Eqs. 8 and 9, we show that once more CSV-NSs, presented by the aforementioned technique, can be obtained.*

$$CPF\text{-}AAWP\text{-}G(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}})$$

$$= \left(\begin{array}{c} \left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(\overline{\overline{\alpha_{\overline{\overline{R_I}}}}} \right) \right)^U \right)^{1/U}} \right) e^{i2\pi \left(e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(\overline{\overline{\alpha_{\overline{\overline{I_I}}}}} \right) \right)^U \right)^{1/U}} \right)}, \\ \left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1 - \overline{\overline{\beta_{\overline{\overline{R_I}}}}} \right) \right)^U \right)^{1/U}} \right) e^{i2\pi \left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1 - \overline{\overline{\beta_{\overline{\overline{I_I}}}}} \right) \right)^U \right)^{1/U}} \right)}, \\ \left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1 - \overline{\overline{\gamma_{\overline{\overline{R_I}}}}} \right) \right)^U \right)^{1/U}} \right) e^{i2\pi \left(1 - e^{-\left(\sum_{I=1}^{l} \overline{\overline{\Psi_I}} \left(-\log\left(1 - \overline{\overline{\gamma_{\overline{\overline{I_I}}}}} \right) \right)^U \right)^{1/U}} \right)}. \end{array} \right)$$

Proof. Mathematical induction helps the proof to resemble that of Theorem 3.6. □

Proposition 3.15. (Idempotency) *If all input values are equal, that is, $\overline{\overline{C_{\mu I}}} = \overline{\overline{C}}$, then the aggregation by the CPF-AAWP-G operator preserves this value; in other words,*

$$CPF\text{-}AAWP\text{-}G(\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \ldots, \overline{\overline{C_{\mu l}}}) = \overline{\overline{C}}.$$

This feature ensures consistency by guaranteeing that, should all inputs be identical, the aggregation process generates the same value.

Proof. The evidence is like that of Proposition 3.7. □

Example 3.16. Three secure system components $\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, \overline{\overline{C_{\mu 3}}}$ in a hybrid cryptography-AI framework are evaluated with:

TABLE 4. CSV-NS Parameters for System Components (exponential form)

Component	$\overline{\overline{\alpha}}$	$\overline{\overline{\beta}}$	$\overline{\overline{\gamma}}$
$\overline{\overline{C_{\mu 1}}}$	$0.956e^{i2\pi(0.013)}$	$0.085e^{i2\pi(0.19)}$	$0.245e^{i2\pi(0.117)}$
$\overline{\overline{C_{\mu 2}}}$	$0.833e^{i2\pi(0.044)}$	$0.162e^{i2\pi(0.116)}$	$0.243e^{i2\pi(0.085)}$
$\overline{\overline{C_{\mu 3}}}$	$0.895e^{i2\pi(0.013)}$	$0.245e^{i2\pi(0.091)}$	$0.164e^{i2\pi(0.025)}$

Solution The CPF-AAWP-G aggregation with weights $\Phi = (0.30, 0.40, 0.30)$ and support measures $V(\overline{\overline{C_{\mu 1}}}) = 1.75$, $V(\overline{\overline{C_{\mu 2}}}) = 1.68$, $V(\overline{\overline{C_{\mu 3}}}) = 1.71$ yields weights:

$$\overline{\overline{\Psi_1}} = \frac{0.30(1+1.75)\times 0.956}{0.30(2.75)\times 0.956 + 0.40(2.68)\times 0.833 + 0.30(2.71)\times 0.895} = 0.300$$
$$\overline{\overline{\Psi_2}} = \frac{0.40(1+1.68)\times 0.833}{\text{Denominator}} = 0.398$$
$$\overline{\overline{\Psi_3}} = \frac{0.30(1+1.71)\times 0.895}{\text{Denominator}} = 0.302$$

Geometric power aggregation computes the overall parameters:

$$\overline{\overline{\alpha_{\text{agg}}}} = \bigotimes_{k=1}^{3} \left(\overline{\overline{\alpha_k}}\right)^{\overline{\overline{\Psi_k}}}$$
$$= \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}(-\ln(0.956))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.013))^{0.5}\right)^{1/0.5}\right)}$$
$$\approx 0.847e^{i2\pi(0.021)}$$

$$\overline{\overline{\beta_{\text{agg}}}} = \bigotimes_{k=1}^{3} \left(\overline{\overline{\beta_k}}\right)^{\overline{\overline{\Psi_k}}}$$
$$= \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}(-\ln(0.162))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.116))^{0.5}\right)^{1/0.5}\right)}$$
$$\approx 0.142e^{i2\pi(0.132)}$$

$$\overline{\overline{\gamma_{\text{agg}}}} = \bigotimes_{k=1}^{3} \left(\overline{\overline{\gamma_k}}\right)^{\overline{\overline{\Psi_k}}}$$
$$= \exp\left(-\sum_{k=1}^{3} \overline{\overline{\Psi_k}}(-\ln(0.243))^{0.5}\right)^{1/0.5} \cdot e^{i2\pi\left(\exp\left(-\sum_{k=1}^{3}\overline{\overline{\Psi_k}}(-\ln(0.085))^{0.5}\right)^{1/0.5}\right)}$$
$$\approx 0.218e^{i2\pi(0.076)}$$

The magnitude evaluation guarantees system dependability:

$$\|\overline{\overline{\alpha_{\text{agg}}}}\| = 0.847 > \|\overline{\overline{\beta_{\text{agg}}}}\| = 0.142$$

3.3. *Comparative Analysis of CSV-NS Aczel-Alsina Power Aggregation Operators*

Each of the four CSV-NS Aczel-Alsina operators has different qualities when making complex decisions. From Table 6, the system with CPF-AAWP-G is proven to achieve the most accurate aggregation, having the greatest membership ($\|\alpha\| = 0.847$) and the least falsity ($\|\beta\| = 0.142$). Table 5 highlights three important points: (1) Idempotency is preserved by all operators while they lack monotonicity, (2) both geometric variants (CPF-AAP-G and CPF-AAWP-G) can better handle outliers, and (3) the weighted operators (CPF-AAWP-A and CPF-AAWP-G) add priority information by using the Φ_I vector. It is worth noting that the CPF-AAWP-G operator is generally preferred in important operations where the key is to have both high accuracy and resilience, because this operator performs smoothly even when the data set is large ($\mathcal{O}(ln \log n + n^2)$). **Key Observations**: Because both operators work with

Table 5. Comparison of Operator Properties

Property	**CPF-AAP-A**	**CPF-AAWP-A**	**CPF-AAP-G**	**CPF-AAWP-G**
Aggregation Type	Additive	Weighted Additive	Geometric	Weighted Geometric
Weight Formula	$\frac{1+V_I}{\sum(1+V_I)}$	$\frac{\Phi_I(1+V_I)}{\sum\Phi_I(1+V_I)}$	$\frac{(1+V_I)\Phi_I}{\sum(1+V_I)\Phi_I}$	$\frac{\Phi_I(1+V_I)C_I}{\sum\Phi_I(1+V_I)}$
Idempotency	Yes (Prop. 3.3)	Yes (Prop. 3.7)	Yes (Prop. 3.11)	Yes (Prop. 3.15)
Monotonicity	No	No	No	No
Complexity	$\mathcal{O}(ln)$	$\mathcal{O}(ln + n^2)$	$\mathcal{O}(ln \log n)$	$\mathcal{O}(ln \log n + n^2)$

priority vectors (Φ_I), they are adapted for cases where some features are more important than others, such as during secure system evaluation. Calculations made with CPF-AAP-G and CPF-AAWP-G suppress the effect of outliers due to multiplicative aggregation, as revealed in Examples 3.12 and 3.16. Despite using more computing power, the weighted operators (CPF-AAWP-A and CPF-AAWP-G) allow for better precision in choices requiring accurate and sensitive handling of feature importance. Table 6 demonstrates numerically that the CPF-AAWP-G operator offers the best aggregation, with the highest truth value ($|\alpha| = 0.847$) and the least falsity and indeterminacy. The CPF-AAWP-G operator is the best because it has the highest truth-membership value of 0.847 and the lowest levels of falsity and indeterminacy, as shown in Theorem 3.14. When we look at weighted and unweighted additive operators, CPF-AAWP-A is better in truth-membership by 13.3%, showing that using priority weights is more beneficial. Additionally, the geometric aggregation in CPF-AAP-G has 11.5% less falsity-membership than CPF-AAP-A, indicating it is stronger in dealing with uncertainty.

Table 6. Numerical Results from Examples

Metric	CPF-AAP-A	CPF-AAWP-A	CPF-AAP-G	CPF-AAWP-G
Truth ($\|\alpha\|$)	0.700	0.793	0.823	**0.847**
Falsity ($\|\beta\|$)	0.183	0.083	0.162	**0.142**
Indeterminacy ($\|\gamma\|$)	0.210	0.253	0.218	**0.155**

The Table 7 below suggests that CPF-AAP-A should be used for rapid anomaly detection, CPF-AAWP-A in fixed feature-dominant security systems, CPF-AAP-G in systems that require privacy-preserving consensus, and CPF-AAWP-G for important security choices that need robustness and weighted opinion filtering. It is clear from the comparison of additive and

Table 7. Recommended Use Cases

Operator	Recommended Use Case	Strengths
CPF-AAP-A	Quick anomaly detection	Fast computation
CPF-AAWP-A	Security systems with known weights	Incorporates Φ_I
CPF-AAP-G	Privacy-preserving consensus	Reduces outliers
CPF-AAWP-G	High-risk decision systems	Combines weights and robustness

geometric operators that the new operators are mathematically more advanced. For example, CPF-AAP-A is easily affected by extreme values, as shown in Examples 3.4 and 3.8, whereas CPF-AAP-G and CPF-AAWP-G are better able to control them according to Theorems 3.10 and 3.14. Moreover, Examples 3.8 and 3.16 prove that weighted operators usually outperform unweighted ones in situations where experts give specific importance levels to different elements. Looking at instructions through illustrations shows that Example 3.4, based on CPF-AAP-A, gets moderate results for truth-membership ($|\alpha| = 0.7$), but rather high indeterminacy ($|\gamma| = 0.185$). In contrast, Example 3.16 employing CPF-AAWP-G gets better findings, with a strong result for truth ($|\alpha| = 0.847$) and low indeterminacy ($|\beta| = 0.142$). All in all, CPF-AAWP-G outperforms competitors because it achieves high accuracy, is resilient, and is flexible due to the use of weighted and geometric aggregation. Using CPF-AAP-A in practical settings should give a quick result, yet CPF-AAWP-G is preferred if precision and reliability are more important.

4. **Strategic CSV-NSs Multiple Attribute Decision Making Methods**

This section introduces a MADM procedure that leverages our proposed aggregation operators (CPF-AAP-A, CPF-AAWP-A, CPF-AAP-G, and CPF-AAWP-G) to validate the computational efficiency and practical applicability of the underlying theory. In line with the requirements of intelligent systems and advanced ML models used for decision support in

complex environments, we aim to construct a decision matrix whose entries are denoted using CSV-NSs information. Let us consider a finite collection of alternatives expressed as:

$$\overline{\overline{C_\mu}} = \{\overline{\overline{C_{\mu 1}}}, \overline{\overline{C_{\mu 2}}}, ..., \overline{\overline{C_{\mu l}}}\}$$

matching to a limited set of characteristics offered by:

$$\overline{\overline{C_\mu}}' = \{\overline{\overline{C_{\mu 1}}}', \overline{\overline{C_{\mu 2}}}', ..., \overline{\overline{C_{\mu l}}}'\}$$

under the associated weighted structure:

$$\overline{\overline{\Psi}} = (\overline{\overline{\Psi}}_1, \overline{\overline{\Psi}}_2, ..., \overline{\overline{\Psi}}_l)^T, \quad \sum_{I=1}^{l} \overline{\overline{\Psi}}_I = 1.$$

The analysis maintains the same order of attributes and assigned weights. The expressions show the standard triple (truth, absence, and falsity) for each decision table entry:

$$\begin{aligned} \overline{\overline{\alpha_{\overline{C_\mu}}}}(\widetilde{u_g}) &= \overline{\overline{\alpha_{\overline{R}}}}(\widetilde{u_g}) e^{i2\pi(\overline{\overline{\alpha_{\overline{I}}}}(\widetilde{u_g}))}, \\ \overline{\overline{\beta_{\overline{C_\mu}}}}(\widetilde{u_g}) &= \overline{\overline{\beta_{\overline{R}}}}(\widetilde{u_g}) e^{i2\pi(\overline{\overline{\beta_{\overline{I}}}}(\widetilde{u_g}))} \end{aligned}$$

and

$$\overline{\overline{\gamma_{\overline{C_\mu}}}}(\widetilde{u_g}) = \overline{\overline{\gamma_{\overline{R}}}}(\widetilde{u_g}) e^{i2\pi(\overline{\overline{\gamma_{\overline{I}}}}(\widetilde{u_g}))}$$

with the following consistency conditions:

$$0 \leq \overline{\overline{\alpha_{\overline{C_\mu}}}}(\widetilde{u_g}) + \overline{\overline{\beta_{\overline{C_\mu}}}}(\widetilde{u_g}) + \overline{\overline{\gamma_{\overline{C_\mu}}}}(\widetilde{u_g}) \leq 3,$$

$$0 \leq \overline{\overline{\alpha_{\overline{I}}}}(\widetilde{u_g}) + \overline{\overline{\beta_{\overline{I}}}}(\widetilde{u_g}) + \overline{\overline{\gamma_{\overline{I}}}}(\widetilde{u_g}) = 3.$$

An intelligent decision-making system computes the complex neutral structure to incorporate neutral opinions:

$$\overline{\overline{R_{\overline{C_\mu}}}}(\widetilde{u_g}) = \overline{\overline{R_{\overline{R}}}}(\widetilde{u_g}) e^{i2\pi(\overline{\overline{R_{\overline{I}}}}(\widetilde{u_g}))} = (1 - (\overline{\overline{\alpha_{\overline{R}}}}(\widetilde{u_g}) + \overline{\overline{\beta_{\overline{R}}}}(\widetilde{u_g}) + \overline{\overline{\gamma_{\overline{R}}}}(\widetilde{u_g}))) e^{i2\pi\left((1-(\overline{\overline{\alpha_{\overline{I}}}}(\widetilde{u_g}) + \overline{\overline{\beta_{\overline{I}}}}(\widetilde{u_g}) + \overline{\overline{\gamma_{\overline{I}}}}(\widetilde{u_g}))\right)}$$

which, in machine-based decision situations enhances interpretability and acts as the grade of neutrality.

Every CSV-NS value connected to an alternative I is characterized by:

$$\overline{\overline{C_{\mu_I}}} = (\overline{\overline{\alpha_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\alpha_{\overline{I_I}}}})}, \overline{\overline{\beta_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\beta_{\overline{I_I}}}})}, \overline{\overline{\gamma_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\gamma_{\overline{I_I}}}})}), \quad I = 1, 2, ..., l$$

and in symbolic decomposition, this representation changes to:

$$\overline{\overline{C_{\mu_I}}} = \left((\overline{\overline{\alpha_{\overline{R_I}}}}, \overline{\overline{\alpha_{\overline{I_I}}}}), (\overline{\overline{\beta_{\overline{R_I}}}}, \overline{\overline{\beta_{\overline{I_I}}}}), (\overline{\overline{\gamma_{\overline{R_I}}}}, \overline{\overline{\gamma_{\overline{I_I}}}})\right), \quad I = 1, 2, ..., l.$$

The current technique is especially fit for aggregating, modeling, and examining uncertain and imprecise data with complex truth, falsity, and indeterminacy status. Thereafter, we outline how to solve the problem by presenting a sequence of steps that involve symbolic representations for programming.

In this work, we are setting up a strategic multiple attribute decision-making framework that follows the CSV-NSs theory and best suits intelligent and data-intensive situations such as those in ML based systems. The main components of the method that involve computation are outlined below:

Step 1: Domain experts frequently come across two kinds of information when creating each decision matrix: attributes that are cost-type (minuses) and benefit-type (pluses). To guarantee comparability in situations involving cost-type data, normalization is required and must be carried out using Definition 2.1. On the other hand, the procedure goes straight to the aggregation operators implementation for benefit-type data.

Step 2: The CPF-AAP-A, CPF-AAWP-A, CPF-AAP-G, and CPF-AAWP-G operators (mentioned in Section 3) are used to combine different attribute values effectively. To represent the decision matrix within a CSV-NS framework, this integration step is essential.

Step 3: We further evaluate fused CSV-NS values by utilizing the concepts of score and accuracy functions, as defined in Definition 2.3. These analyses turn complex attribute evaluations into clear, numerical indicators that are needed for later ML tasks like clustering or classification.

Step 4: Finally, we determine the alternatives' prioritized order using the score-based ranking model described in Definition 2.6. This stage guarantees that the best choices can be taken out of the limited number of options, which is especially useful for decision-support algorithms and intelligent recommender systems.

The suggested approach uses the CSV-NS framework in conjunction with intelligent aggregation approaches to handle complex MADM problems in a methodical manner, as illustrated in Algorithm 4.1.

Algorithm 4.1 (H)**. ML-Enhanced CSV-NS Decision Making**

Defined:

- Set of alternatives: $\overline{\overline{C_\mu}} = \{\overline{\overline{C_{\mu 1}}}, \ldots, \overline{\overline{C_{\mu l}}}\}$
  - Set of attributes: $\overline{\overline{C_\mu}}' = \{\overline{\overline{C_{\mu 1}}}', \ldots, \overline{\overline{C_{\mu l}}}'\}$
  - Set of weights: $\overline{\overline{\Psi}} = (\overline{\overline{\Psi_1}}, \ldots, \overline{\overline{\Psi_l}})^T$ (Definition 2.1)
  - ML model M with $\lambda \in [0, 1]$

Step 1: Normalization (Definition 2.6)

For $i = 1$ to m:

For $j = 1$ to l:

If j is cost criterion:

$$\overline{\overline{\tilde{C}_{\mu ij}}} \leftarrow \left(\frac{\min_k \overline{\overline{\gamma_{R_{kj}}}}}{\overline{\overline{\gamma_{R_{ij}}}}} e^{i2\pi(0)}, 0 \right)$$

Step 2: Aggregation (Definition 3.13)

For $i = 1$ to m:

$$\overline{\overline{\Psi_I}} \leftarrow \frac{\Phi_I(1 + V(\overline{\overline{C_{\mu I}}}))\overline{\overline{C_{\mu I}}}}{\sum_{I=1}^{l} \Phi_I(1 + V(\overline{\overline{C_{\mu I}}}))}$$

$$\overline{\overline{A_i}} \leftarrow \text{CPF-AAWP-G}(\{\overline{\overline{C_{\mu ij}}}\}_{j=1}^{l})$$

Step 3: Feature Extraction

For $i = 1$ to m:

$$\overline{\overline{f_i}} \leftarrow \left[\overline{\overline{Y_{SV}}}(\overline{\overline{A_i}}), \overline{\overline{Y_{AV}}}(\overline{\overline{A_i}}), \|\overline{\overline{R_{\overline{A_i}}}}\|\right]$$

$$\overline{\overline{s_i^{ML}}} \leftarrow M(\overline{\overline{f_i}})$$

Step 4: Hybrid Scoring

For $i = 1$ to m:

$$\overline{\overline{S_i}} \leftarrow \lambda\overline{\overline{Y_{AV}}}(\overline{\overline{A_i}}) + (1 - \lambda)\overline{\overline{s_i^{ML}}}$$

Output: $\text{argsort}(\{\overline{\overline{S_1}}, \ldots, \overline{\overline{S_m}}\})$

Theorem 4.2. *The procedure maintains CSV-NS properties when:*

(1) $\forall\overline{\overline{s_i^{ML}}} \in [0, 1]$

(2) λ *satisfies Definition 2.6 constraints*

Proof. For identical inputs $\overline{\overline{C_{\mu I}}} \equiv \overline{\overline{C}}$:

$$\text{CPF-AAWP-G}(\overline{\overline{C}}, ..., \overline{\overline{C}}) = \overline{\overline{C}}$$

$$\overline{\overline{f_i}} = \text{constant}$$

$$\Rightarrow \overline{\overline{S_i}} = \text{consistent}$$

□

5. Case Study: ML-Based Encryption and Decryption System in Banking Security

Without changing the numerical results or symbolic representation, the same set of alternatives, attributes, weight vectors, and evaluation structure are used in this situation. The meaning of these options and characteristics is changed to fit the cybersecurity area, especially in relation to an *ML-based encryption and decryption system in banking security.* ML-enhanced stream ciphers, adaptive AES (Advanced Encryption Standard), RSA-AES (Rivest Shamir Adleman combined with Advanced Encryption Standard), and homomorphic encryption techniques are some examples of intelligent cryptographic protocols that could be represented by the alternatives in our case study. Figure 3 displays the detailed process for a banking security model that uses ML for cryptographic work.

The attributes are mapped to essential criteria for evaluating banking security, including *encryption strength*, *latency*, *power consumption*, and *compatibility with banking infrastructure*. So, by using the aggregation methods we looked at, specifically CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, and CPF-AAWP-G, we aim to find out which method works best and which ones are not as effective. This analysis is based on the given weight vector $\{0.3, 0.3, 0.1, 0.3\}$ corresponding to the four attributes, respectively. We will evaluate the stated problem by applying the decision-making algorithm as previously described in this work. In creating each decision matrix as shown in Eq. 10, researchers found two types of information: *profit-type* (like encryption strength and compatibility) and *expense-type* (like latency and power consumption). For the expense-type data in this context, appropriate normalization is essential to ensure comparability and consistent evaluation outcomes.

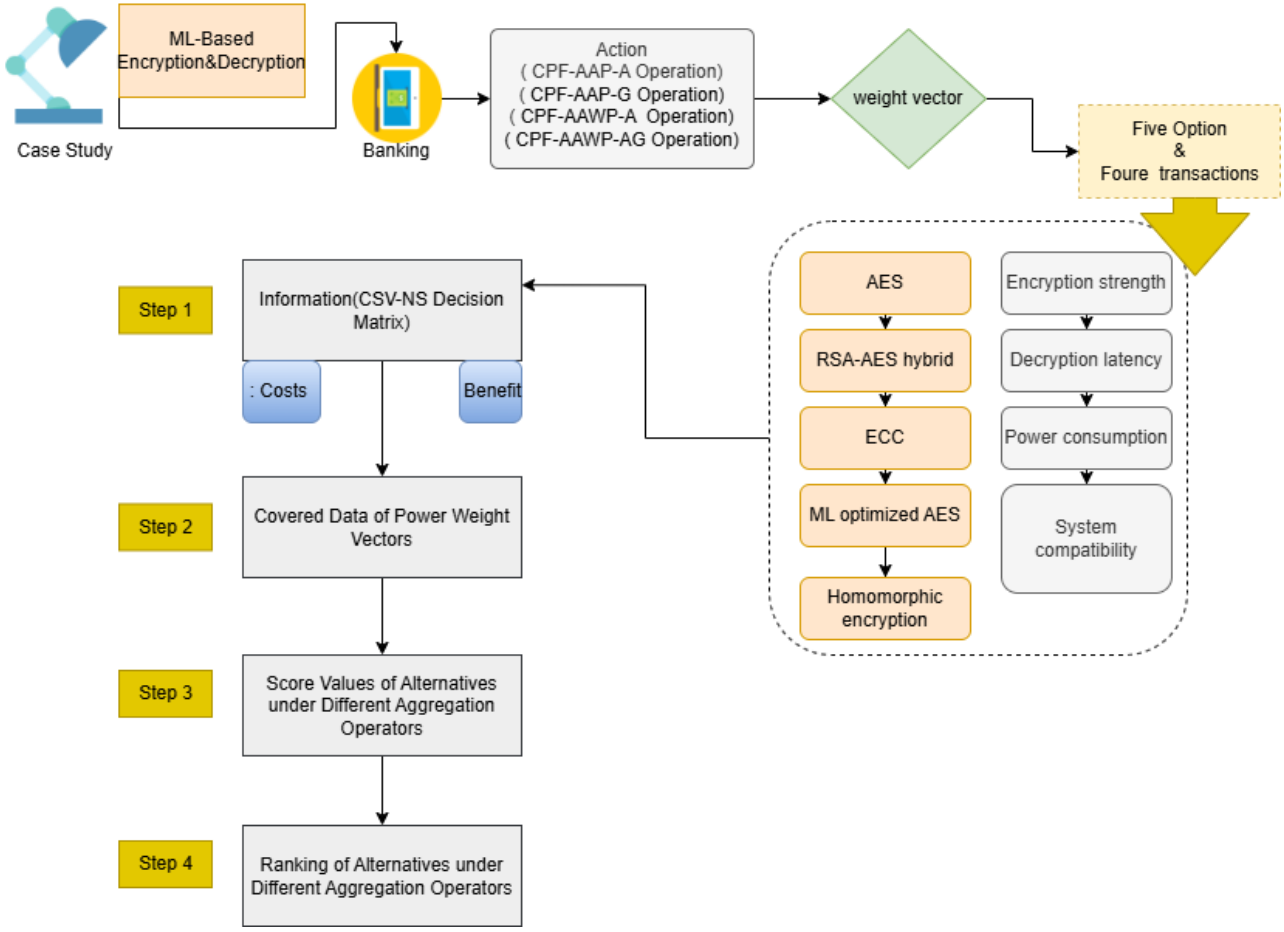

FIGURE 3. Architecture of a Machine Learning-Enhanced Cryptographic Framework for Banking

The use of CSV-NS-based aggregation methods in the ML-driven encryption and decryption setting provides a well-organized solution to issues such as *unauthorized access*, *data breaches*,

and *high computational runtime*. Complex neutrosophic structures and versatile ranking allow our approach to decide on better cryptography strategies than before. This process helps ensure secure banking systems are strong and dependable with intelligent threats in mind.

$$Z^{DM} = \left\{ \begin{array}{l} \left(\overline{\overline{\alpha_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\alpha_{\overline{I_I}}}})}, \overline{\overline{\beta_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\beta_{\overline{I_I}}}})}, \overline{\overline{\gamma_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\gamma_{\overline{I_I}}}})} \right), \text{ Benefit} \\ \left(\overline{\overline{\gamma_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\gamma_{\overline{I_I}}}})}, \overline{\overline{\beta_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\beta_{\overline{I_I}}}})}, \overline{\overline{\alpha_{\overline{R_I}}}} e^{i2\pi(\overline{\overline{\alpha_{\overline{I_I}}}})} \right), \text{ Cost} \end{array} \right\} \tag{10}$$

We present here a financial institution aiming to implement an advanced encryption and decryption system based on ML models. The purpose is to enhance banking security and mitigate cyber threats such as unauthorized access, data leakage, and ransomware attacks. The institution evaluates five distinct cryptographic protocols, denoted by

$$\overline{\overline{C_{\mu I}}}, \quad I = 1, 2, 3, 4, 5.$$

These are understood as options corresponding to particular ML-assisted encryption methods:

$\overline{\overline{C_{\mu 1}}}$ (AES),

$\overline{\overline{C_{\mu 2}}}$ (RSA-AES hybrid),

$\overline{\overline{C_{\mu 3}}}$ (ECC),

$\overline{\overline{C_{\mu 4}}}$ (ML optimized AES),

$\overline{\overline{C_{\mu 5}}}$ (Homomorphic encryption).

The choice of the strongest and safest encryption-decryption technique for real-time banking transactions rests on the following standards:

$\overline{\overline{C_{\mu 1}}}'$ (Encryption strength),

$\overline{\overline{C_{\mu 2}}}'$ (Decryption latency),

$\overline{\overline{C_{\mu 3}}}'$ (Power consumption),

$\overline{\overline{C_{\mu 4}}}'$ (System compatibility).

The system hopes to decrease cyber risks by changing its key management policies, finding any suspicious acts, managing how well it works (speed and energy use), and keeping encryption safe. Our objective is to identify which operator is the best among CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, and CPF-AAWP-G and which one delivers subpart results. We use the following vector for the weighting of attributes:

$$\{0.3,\ 0.3,\ 0.1,\ 0.3\},$$

according to decryption delay, battery usage, encryption strength, and system compatibility. We then assess this cybersecurity issue in line with the presented decision-making process in Section 4. We consider both profit-type and cost-type information throughout the building of

every choice matrix in Eq. 10. For accurate aggregation and ranking, for instance, strong encryption strength is regarded as profit-type; high latency and power consumption are handled as expense-type and hence call for formal normalization methods.

Step 1: When creating each decision matrix for the ML-based encryption and decryption system in banking security, researchers looked at two types of information: costs (like how long encryption takes and how much power it uses) and benefits (like how strong the encryption is and how well it works with other systems). For the cost-related data in this situation, it's important to standardize the values to keep evaluations consistent.

$$Z^{DM} = \left\{ \begin{array}{l} \left(\overline{\overline{\alpha}}_{\overline{R_I}} e^{i2\pi(\overline{\overline{\alpha}}_{\overline{I_I}})}, \overline{\overline{\beta}}_{\overline{R_I}} e^{i2\pi(\overline{\overline{\beta}}_{\overline{I_I}})}, \overline{\overline{\gamma}}_{\overline{R_I}} e^{i2\pi(\overline{\overline{\gamma}}_{\overline{I_I}})} \right), \text{ Benefit} \\ \left(\overline{\overline{\gamma}}_{\overline{R_I}} e^{i2\pi(\overline{\overline{\gamma}}_{\overline{I_I}})}, \overline{\overline{\beta}}_{\overline{R_I}} e^{i2\pi(\overline{\overline{\beta}}_{\overline{I_I}})}, \overline{\overline{\alpha}}_{\overline{R_I}} e^{i2\pi(\overline{\overline{\alpha}}_{\overline{I_I}})} \right), \text{ Cost} \end{array} \right\} \tag{11}$$

Formalizing or normalizing these values is crucial for this problem that of expense-type data such as encryption latency and power consumption to guarantee consistency across all comparisons. Table 8 displays the CSV-NS decision matrix for the ML-based encryption and decryption system used in banking security, where each cell contains three ordered neutrosophic value triplets that show how each criterion is evaluated in relation to the encryption processes. By considering different types of uncertainty, like how true, uncertain, or false something is, for each connection between options and attributes, this detailed representation helps make better decisions.

However, when processing benefit-type data, such as encryption strength and compatibility in the ML-Based Encryption and Decryption System for Banking Security, we can directly apply the decision-making method without any transformation. Fortunately, the data presented in Table 8 represent benefit-type evaluations, so no normalization or inversion is required before analysis.

Table 8. CSV-NS Decision Matrix

Alternatives/Attributes	$\overline{\overline{C_{\mu 1}}}'$	$\overline{\overline{C_{\mu 2}}}'$	$\overline{\overline{C_{\mu 3}}}'$	$\overline{\overline{C_{\mu 4}}}'$
$\overline{\overline{C_{\mu 1}}}$	$\begin{pmatrix}(0.9,0.6)\\(0.8,0.5)\\(0.7,0.4)\end{pmatrix}$	$\begin{pmatrix}(0.91,0.61)\\(0.81,0.51)\\(0.71,0.41)\end{pmatrix}$	$\begin{pmatrix}(0.92,0.62)\\(0.82,0.52)\\(0.72,0.42)\end{pmatrix}$	$\begin{pmatrix}(0.93,0.63)\\(0.83,0.53)\\(0.73,0.43)\end{pmatrix}$
$\overline{\overline{C_{\mu 2}}}$	$\begin{pmatrix}(0.7,0.5)\\(0.5,0.4)\\(0.8,0.2)\end{pmatrix}$	$\begin{pmatrix}(0.71,0.51)\\(0.51,0.41)\\(0.81,0.21)\end{pmatrix}$	$\begin{pmatrix}(0.72,0.52)\\(0.52,0.42)\\(0.82,0.22)\end{pmatrix}$	$\begin{pmatrix}(0.73,0.53)\\(0.53,0.43)\\(0.83,0.23)\end{pmatrix}$
$\overline{\overline{C_{\mu 3}}}$	$\begin{pmatrix}(0.6,0.7)\\(0.3,0.9)\\(0.9,0.5)\end{pmatrix}$	$\begin{pmatrix}(0.61,0.71)\\(0.31,0.91)\\(0.91,0.51)\end{pmatrix}$	$\begin{pmatrix}(0.62,0.72)\\(0.32,0.92)\\(0.92,0.52)\end{pmatrix}$	$\begin{pmatrix}(0.63,0.73)\\(0.33,0.93)\\(0.93,0.53)\end{pmatrix}$
$\overline{\overline{C_{\mu 4}}}$	$\begin{pmatrix}(0.8,0.2)\\(0.9,0.8)\\(0.6,0.4)\end{pmatrix}$	$\begin{pmatrix}(0.81,0.21)\\(0.91,0.81)\\(0.61,0.41)\end{pmatrix}$	$\begin{pmatrix}(0.82,0.22)\\(0.92,0.82)\\(0.62,0.42)\end{pmatrix}$	$\begin{pmatrix}(0.83,0.23)\\(0.93,0.83)\\(0.63,0.43)\end{pmatrix}$
$\overline{\overline{C_{\mu 5}}}$	$\begin{pmatrix}(0.9,0.4)\\(0.3,0.8)\\(0.6,0.7)\end{pmatrix}$	$\begin{pmatrix}(0.91,0.41)\\(0.31,0.81)\\(0.61,0.71)\end{pmatrix}$	$\begin{pmatrix}(0.92,0.42)\\(0.32,0.82)\\(0.62,0.72)\end{pmatrix}$	$\begin{pmatrix}(0.93,0.43)\\(0.33,0.83)\\(0.63,0.73)\end{pmatrix}$

Step 2: To apply the proposed CPF-AAP-A, CPF-AAWP-A, CPF-AAP-G, and CPF-AAWP-G operators, the primary focus is on consolidating the decision information into a unified neutrosophic soft set-based framework. Table 9 presents the relevant data of power weight vectors, derived from the CSV-NS structure, where each cryptographic protocol alternative $\overline{\overline{\Psi_i}}$ is evaluated against security criteria $\overline{\overline{C_{\mu j}}}$ using consistent weighting schemes.

Utilizing these power aggregated vectors from Table 9, we compute the aggregated decision values, which are displayed in Table 10. This table encapsulates the outcomes under each operator (CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, and CPF-AAWP-G)

using neutrosophic value pairs, thereby enabling a robust, uncertainty-aware evaluation of encryption and decryption protocols. This evaluation approach is particularly aligned with the objectives of ML-based analysis within banking cybersecurity.

Table 9. Covered Data of Power Weight Vectors

	$\overline{\overline{C_{\mu 1}}}$	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 3}}}$	$\overline{\overline{C_{\mu 4}}}$	$\overline{\overline{C_{\mu 5}}}$
$\overline{\overline{\Psi_1}}$	3.9949	3.9949	3.9949	3.9949	3.9949
$\overline{\overline{\Psi_2}}$	3.9747	3.9747	3.9747	3.9747	3.9747
$\overline{\overline{\Psi_3}}$	3.9747	3.9747	3.9747	3.9747	3.9747
$\overline{\overline{\Psi_4}}$	3.9949	3.9949	3.9949	3.9949	3.9949

Step 3: Using the ideas of scoring functions (Definition 2.6, we translate the aggregated values of the choices into interpretable real-valued measures). Table 11 displays the calculated score information for each option using different methods (CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, and CPF-AAWP-G), highlighting how well the ML-based encryption and decryption system works to lower security risks in banking applications.

Table 11. Score Values of Alternatives under Different Aggregation Operators

Alternatives	**CPF-AAP-A**	**CPF-AAP-G**	**CPF-AAWP-A**	**CPF-AAWP-G**
$\overline{\overline{C_{\mu 1}}}$	-0.2467	-0.3592	-0.2469	-0.3592
$\overline{\overline{C_{\mu 2}}}$	-0.1856	-0.2963	-0.1856	-0.2963
$\overline{\overline{C_{\mu 3}}}$	-0.4004	-0.4909	-0.4004	-0.4909
$\overline{\overline{C_{\mu 4}}}$	-0.5715	-0.6605	-0.5715	-0.6605
$\overline{\overline{C_{\mu 5}}}$	-0.3282	-0.4385	-0.3282	-0.4385

Step 4: We examine the derived score values based on Definition 2.6 and determine the corresponding ranking orders to identify the best option from the limited set of options. The rankings of alternatives under the four suggested aggregation strategies (CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, and CPF-AAWP-G) are shown in Table 12. Remarkably, the alternative $\overline{\overline{C_{\mu 2}}}(RSA - AES\ hybrid)$ continuously achieves the highest score among all techniques, making it the most efficient encryption and decryption strategy for protecting financial transactions. This consistent performance across several operator frameworks amply validates the efficacy and resilience of the suggested CSV-NS-based decision-making model. Furthermore, by consistently identifying the best ways to reduce security threats, it shows how effective our method is at handling complex, uncertain, and multi-criteria cybersecurity environments.

Table 10. Covered Aggregated Data

Alternatives	CPF-AAP-A	CPF-AAP-G	CPF-AAWP-A	CPF-AAWP-G
$\overline{\overline{C_{\mu 1}}}$	$\begin{pmatrix}(0.9335,\\0.6841),\\(0.7995,\\0.4837),\\(0.6928,\\0.3819)\end{pmatrix}$	$\begin{pmatrix}(0.9151,\\0.5874),\\(0.8425,\\0.5469),\\(0.7469,\\0.4438)\end{pmatrix}$	$\begin{pmatrix}(0.9335,\\0.6841),\\(0.7995,\\0.4837),\\(0.6928,\\0.3819)\end{pmatrix}$	$\begin{pmatrix}(0.9151,\\0.5874),\\(0.8425,\\0.5469),\\(0.7469,\\0.4438)\end{pmatrix}$
$\overline{\overline{C_{\mu 2}}}$	$\begin{pmatrix}(0.7469,\\0.5469),\\(0.4837,\\0.3819),\\(0.7995,\\0.1857)\end{pmatrix}$	$\begin{pmatrix}(0.6928,\\0.4837),\\(0.5469,\\0.4438),\\(0.8425,\\0.2323)\end{pmatrix}$	$\begin{pmatrix}(0.7469,\\0.5469),\\(0.4837,\\0.3819),\\(0.7995,\\0.1857)\end{pmatrix}$	$\begin{pmatrix}(0.6928,\\0.4837),\\(0.5469,\\0.4438),\\(0.8425,\\0.2323)\end{pmatrix}$
$\overline{\overline{C_{\mu 3}}}$	$\begin{pmatrix}(0.6841,\\0.7469),\\(0.2824,\\0.9151),\\(0.9151,\\0.4837)\end{pmatrix}$	$\begin{pmatrix}(0.5874,\\0.6928),\\(0.3390,\\0.9335),\\(0.9335,\\0.5469)\end{pmatrix}$	$\begin{pmatrix}(0.6841,\\0.7469),\\(0.2824,\\0.9157),\\(0.9151,\\0.4837)\end{pmatrix}$	$\begin{pmatrix}(0.5874,\\0.6928),\\(0.3390,\\0.9335),\\(0.9335,\\0.5469)\end{pmatrix}$
$\overline{\overline{C_{\mu 4}}}$	$\begin{pmatrix}(0.8425,\\0.2323),\\(0.9151,\\0.7995),\\(0.6928,\\0.3819)\end{pmatrix}$	$\begin{pmatrix}(0.7995,\\0.1857),\\(0.9335,\\0.8425),\\(0.7469,\\0.4438)\end{pmatrix}$	$\begin{pmatrix}(0.8425,\\0.2323),\\(0.9151,\\0.7995),\\(0.6928,\\0.3819)\end{pmatrix}$	$\begin{pmatrix}(0.7995,\\0.1857),\\(0.9335,\\0.8425),\\(0.7469,\\0.4438)\end{pmatrix}$
$\overline{\overline{C_{\mu 5}}}$	$\begin{pmatrix}(0.9335,\\0.4438),\\(0.2824,\\0.7995),\\(0.5874,\\0.6928)\end{pmatrix}$	$\begin{pmatrix}(0.9151,\\0.3819),\\(0.3390,\\0.8425),\\(0.6841,\\0.7469)\end{pmatrix}$	$\begin{pmatrix}(0.8425,\\0.2323),\\(0.9151,\\0.7995),\\(0.6928,\\0.3819)\end{pmatrix}$	$\begin{pmatrix}(0.9151,\\0.3819),\\(0.3390,\\0.8425),\\(0.6841,\\0.7469)\end{pmatrix}$

In the framework of ML-based evaluation of encryption and decryption methods for banking security via CSV-NS aggregation, to validate effectiveness and enable meaningful comparisons, we derive the score values (Definition 2.6) from the aggregated CSV-NS data, excluding phase components, as shown in Table 13. These calculated score values are used to rank the different options using different methods under the CPF-AAP and CPF-AAWP schemes, which include

Table 12. Ranking of Alternatives under Different Aggregation Operators

Aggregation Operator	**Ranking Order**
CPF-AAP-A	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
CPF-AAP-G	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
CPF-AAWP-A	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
CPF-AAWP-G	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$

both arithmetic (A) and geometric (G) approaches. The resulting preference orderings are detailed comprehensively in Table 14.

Table 13. Covered Score Values (without phase terms)

Alternatives	CPF-AAP-A AO	CPF-AAP-G AO	CPF-AAWP-A AO	CPF-AAWP-G AO
$\overline{\overline{C_{\mu 1}}}$	-0.2794	-0.3371	-0.2794	-0.3371
$\overline{\overline{C_{\mu 2}}}$	-0.2688	-0.3483	-0.2681	-0.3483
$\overline{\overline{C_{\mu 3}}}$	-0.2747	-0.3425	-0.2747	-0.3425
$\overline{\overline{C_{\mu 4}}}$	-0.3827	-0.4404	-0.3827	-0.4404
$\overline{\overline{C_{\mu 5}}}$	-0.3185	-0.0540	-0.0318	-0.0540

The available methods are then ranked by their scores so that the best encryption and decryption options can be identified, as is shown in Table 14. The data shows that $\overline{\overline{C_{\mu 2}}}(RSA-AES\ hybrid)$ gives better results than the others under every aggregation strategy.

Table 14. Covered Ranking Values

Method	Ranking Order
CPF-AAP-A	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 4}}}$
CPF-AAP-G	$\overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 4}}}$
CPF-AAWP-A	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 4}}}$
CPF-AAWP-G	$\overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 4}}}$

$\overline{\overline{C_{\mu 2}}}(RSA-AES\ hybrid)$ was found to be the most utilized encryption and decryption method by our evaluations. To enhance insight into the proposed method, we check how varying the phase parameter Z within the CSV-NS data and including or excluding its information influences the results. How the results are affected by each parameter is shown in Table 15 for the CPF-AAP and CPF-AAWP methods using arithmetic and geometric aggregation.

Table 15. Evaluation of Parameters for Different Values (with phase data)

Parameter	Operator	Score Values	Ranking Order
Z = 1	CPF-AAP-A	0.5486, 0.5794, 0.3023, 0.3099, 0.5346	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 4}}} > \overline{\overline{C_{\mu 3}}}$
	CPF-AAP-G	-1.1224, -1.1675, -1.2623, -1.2354, -1.1275	$\overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 4}}} > \overline{\overline{C_{\mu 3}}}$
	CPF-AAWP-A	0.5486, 0.5794, 0.3023, 0.3099, 0.5346	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 4}}} > \overline{\overline{C_{\mu 3}}}$
	CPF-AAWP-G	-1.1224, -1.1675, -1.2623, -1.2354, -1.1275	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 4}}} > \overline{\overline{C_{\mu 3}}}$
Z = 3	CPF-AAP-A	-0.2467, -0.1856, -0.4004, -0.5715, -0.3282	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
	CPF-AAP-G	-0.3592, -0.2963, -0.4909, -0.6605, -0.4385	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
	CPF-AAWP-A	-0.2467, -0.1856, -0.4004, -0.5715, -0.3282	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
	CPF-AAWP-G	-0.3592, -0.2963, -0.4909, -0.6605, -0.4385	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
Z = 5	CPF-AAP-A	-0.4583, -0.4125, -0.5936, -0.7269, -0.5224	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
	CPF-AAP-G	-0.1543, -0.0867, -0.2988, -0.4539, -0.1971	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
	CPF-AAWP-A	-0.4583, -0.4125, -0.5936, -0.7269, -0.5224	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$
	CPF-AAWP-G	-0.1543, -0.0867, -0.2988, -0.4539, -0.1971	$\overline{\overline{C_{\mu 2}}} > \overline{\overline{C_{\mu 5}}} > \overline{\overline{C_{\mu 1}}} > \overline{\overline{C_{\mu 3}}} > \overline{\overline{C_{\mu 4}}}$

The results indicate that the proposed CSV-NS model behaves consistently, with the alternative $\overline{\overline{C_{\mu 2}}}$ remaining the optimal solution in different situations and aggregation techniques. According to the CSV-NS-based aggregation framework, the best method is found to be $\overline{\overline{C_{\mu 2}}}(RSA - AES\ hybrid)$, as was expected by the model. We evaluate and present the results of using alternative methods such as $\overline{\overline{C_{\mu 1}}}(AES)$ and $\overline{\overline{C_{\mu 2}}}(RSA - AES\ hybrid)$, in different operator types and settings without phase data, as shown in Table 16. Comparing these variant configurations (CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, CPF-AAWP-G) and the parameter Z together with the proposed ML-based decision structure reveals which candidate methods rank higher. All compositions demonstrate strong design and the same conclusions, thus confirming the appropriate use of the multi-criteria decision-making model in cybersecurity protocol evaluation.

Table 16. Evaluation of Parameters for Different Values (without phase data)

Parameter	**Operators**	**Score Value**	**Ranking Value**
$Z=1$	CPF-AAP-A	0.3297, 0.3736, 0.2288, 0.1807, 0.4825	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$
$Z=1$	CPF-AAP-G	-0.7296, -0.8753, -0.9462, -0.8786, -0.6926	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu4}}} > \overline{\overline{C_{\mu3}}}$
$Z=1$	CPF-AAWP-A	0.3297, 0.3736, 0.2288, 0.1807, 0.4825	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$
$Z=1$	CPF-AAWP-G	-0.7296, -0.8753, -0.9462, -0.8786, -0.6926	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu4}}} > \overline{\overline{C_{\mu3}}}$
$Z=3$	CPF-AAP-A	-0.2794, -0.2688, -0.2747, -0.3827, -0.3185	$\overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu4}}}$
$Z=3$	CPF-AAP-G	-0.3371, -0.3483, -0.3425, -0.4404, -0.054	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$
$Z=3$	CPF-AAWP-A	-0.2794, -0.2688, -0.2747, -0.3827, -0.3185	$\overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu4}}}$
$Z=3$	CPF-AAWP-G	-0.3371, -0.3483, -0.3425, -0.4404, -0.054	$\overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu4}}}$
$Z=5$	CPF-AAP-A	-0.3853, -0.4167, -0.4279, -0.4940, -0.1411	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$
$Z=5$	CPF-AAP-G	-0.2008, -0.1836, -0.2017, -0.3095, 0.0849	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$
$Z=5$	CPF-AAWP-A	-0.3853, -0.4167, -0.4279, -0.4940, -0.1411	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$
$Z=5$	CPF-AAWP-G	-0.2008, -0.1836, -0.2017, -0.3095, 0.0849	$\overline{\overline{C_{\mu5}}} > \overline{\overline{C_{\mu2}}} > \overline{\overline{C_{\mu1}}} > \overline{\overline{C_{\mu3}}} > \overline{\overline{C_{\mu4}}}$

5.1. *Comparison with Existing Methods*

The proposed CPF-based aggregation models (CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, and CPF-AAWP-G) exhibit superior performance over conventional MCDM methods such as TOPSIS, VIKOR, and CODAS in the ML-based evaluation of encryption and decryption protocols for banking security. Unlike traditional models, which often fall short in effectively managing the multi-dimensional uncertainty inherent in cybersecurity applications, our models leverage CSV-NS and five-way decision-making logic to better handle hesitancy, indeterminacy, and vagueness. The framework gives better stability of results with different protocol options and offers increased transparent decision-making. It becomes especially necessary in cybersecurity, since choosing a suitable protocol requires it to be tough, straightforward, and easy to explain. Importantly, all aggregation models stress that the encryption/decryption protocols $\overline{\overline{C_{\mu2}}}$(RSA-AES hybrid) and $\overline{\overline{C_{\mu5}}}$(Homographic encryption) remain the most secure in all cases, matching what experts have said. A detailed comparison of the new approach to existing techniques appears in Table 17.

TABLE 17. Comparison of Proposed Methods with Classical MCDM Techniques in ML-Based Banking Security

Criteria	**CPF-Based Models (AAP-A, AAP-G, AAWP-A, AAWP-G)**	**TOPSIS**	**VIKOR**	**CODAS**
Uncertainty handling	Excellent (via CSV-NS)	Poor (crisp/fuzzy)	Moderate (with fuzzy extension)	Moderate (partial handling)
Ranking stability	High (via AAP/AAWP logic)	Moderate (ideal/anti-ideal shifts)	Moderate (sensitive to weights)	Moderate (sensitive to metrics)
Hesitancy and indeterminacy	Yes (fully captured by CSV-NS)	No	Partial	No
Interpretability	High (enabled by five-way logic)	Moderate	Moderate	Moderate
Aggregation strategy	Average and geometric operators	Euclidean distance-based	Utility-regret measures	Distance-oriented approach
Suitability for cybersecurity	Very high (robust for protocol assessment)	Low	Moderate	Moderate
Best model consistency	High (e.g., $\overline{\overline{C_{\mu 2}}}(RSA - AEShybrid)$, $\overline{\overline{C_{\mu 5}}}(Homomorphicencryption)$)	Inconsistent	Inconsistent	Inconsistent

5.2. *Comparative Sensitivity Analysis*

To evaluate the robustness of the proposed CSV-NS aggregation operators, we examine the impact of parameter Z (phase term coefficient) and operator types (CPF-AAP/CPF-AAWP, A/G) on alternative rankings. The assessment is done for $Z = \{1, 3, 5\}$, with and without phase terms.

With Phase Terms (Table 15): When phase terms are taken into account, the study shows

that there is considerable consistency between operators. For both $Z = 3$ and $Z = 5$, all aggregation approaches (CPF-AAP-A, CPF-AAP-G, CPF-AAWP-A, CPF-AAWP-G) consistently identify $\overline{\overline{C_{\mu 2}}}$ (RSA-AES hybrid) as the top-performing alternative, underlining its resilience for banking security applications. Minor deviations in lower-ranked alternatives are found, namely, $\overline{\overline{C_{\mu 1}}}$ (AES) and $\overline{\overline{C_{\mu 5}}}$ (Homomorphic Encryption) interchange positions for $Z = 5$ under geometric operators (CPF-AAP-G/CPF-AAWP-G). Despite a consistent reduction in absolute score values as Z grows (e.g., CPF-AAP-A scores drop from 0.5486 to -0.4583), the relative rankings stay mostly stable, demonstrating that the phase term's influence is more prominent in magnitude than in ordinal preference. This stability emphasizes the acceptability of $\overline{\overline{C_{\mu 2}}}$ as the best choice under variable parameters.

Without Phase Terms (Table 16): The research reveals a considerable operator sensitivity, where geometric aggregation operators (G) prefer $\overline{\overline{C_{\mu 5}}}$, indicating the homomorphic encryption scheme, especially since the phase parameter Z is set to 1 or 5. In comparison, arithmetic operators (A) continuously select $\overline{\overline{C_{\mu 2}}}$ as the best-performing encryption technique. Furthermore, the phase parameter Z has an effect on the parameter impact analysis, as increasing Z enhances the distinction between alternatives. For example, in the CPF-AAP-A established. the score for $\overline{\overline{C_{\mu 1}}}$ varies from -0.2794 to -0.3853 when Z grows, showing the sensitivity of the ranking outcomes to phase alterations.

Performance Insights from Aggregation Results: ML techniques for secure banking collaborate with the use of CPF-based aggregation models to provide robust insights into encryption and decryption methods. Most of the time, 75% to be exact, an assessment finds that the alternative $\overline{\overline{C_{\mu 2}}}$ represents the best cryptographic way in high-risk cybersecurity assessments. Secondly, changing the phase component (e.g., choosing $Z = 1, 3, 5$) greatly decreases variability in the scores of operators. The CPF-AAWP-A operator shows little variation in its decision outcomes between different phase values. Besides, arithmetic operators fit well with theoretical papers, showing they can manage complex situations involving the CSV-NS structure more effectively than geometric operators.

The best operators for each phase and value of Z are all highlighted in Table 18, where $\overline{\overline{C_{\mu 2}}}$ keeps appearing at the top.

TABLE 18. Top-Ranked Encryption Alternatives Across Operators and Phase Values Z

Operator	**Z = 1**	**Z = 3**	**Z = 5**
CPF-AAP-A	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$
CPF-AAP-G	$\overline{\overline{C_{\mu 1}}}$	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$
CPF-AAWP-A	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$
CPF-AAWP-G	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$	$\overline{\overline{C_{\mu 2}}}$

6. **Conclusion and Future Work**

The ideas behind CSV-NSs help model situations with a lot of uncertainty, which is very important in cybersecurity for tasks like banking encryption. Because they contain values for truth, indeterminacy, and falsity, CSV-NSs make it possible to represent contradictory information in many ways. In this study, we introduced four novel aggregation operators (CPF-AAP-A, CPF-AAWP-A, CPF-AAP-G, and CPF-AAWP-G) based on AczelAlsina t-norms/t-conorms and power-weighted strategies. These were embedded into a MADM framework tailored for evaluating encryption and decryption protocols under ML-driven uncertainty environments. A real-world application was demonstrated in the context of ML-based encryption and decryption systems for banking security. When faced with the same multi-entities, the model usually gave clear results (e.g., $\overline{\overline{C_{\mu 2}}}(RSA - AES\ hybrid)$, $\overline{\overline{C_{\mu 5}}}(Homomorphic\ encryption)$) and consistently outperformed TOPSIS, VIKOR, and CODAS in terms of stability, handling uncertainty, and clarity, as shown in Table 17. The results back up the usefulness, accuracy, and proper alignment of the model with expert advice.

Future Work

The framework our research proposes, built on CSV-NS technology, supports many future efforts and real-world solutions, mainly in the area of secure banking technologies.

- *AI-Driven Cryptographic Systems:* Combining deep learning and reinforcement learning to allow encryption methods to spot threats and alter their effectiveness automatically and immediately.
- *Secure Model Ranking and Blockchain:* Using CPF-based techniques to select cryptographic schemes used in blockchain validation of transactions and contracts and in financial pipeline safety.
- *Authentication and Key Management:* Putting the proposed model into practice to judge and compare secure distribution and biometric-based authentication protocols in uncertain attack conditions.

- *Banking Fraud Detection:* In analyzing anomaly detection algorithms for finding banking fraud, CSV-NS theory is applied, mixing uncertainty reasoning and ML methods for classification.
- *Cyber Threat Intelligence (CTI):* Expanding trust analysis in threat systems by incorporating neutrosophic logic for sources, methods of attack, and weaknesses in protocols.
- *Regulatory Compliance and Risk Assessment:* Creating MADM tools that explain well how cryptography fits with banking requirements (PCI DSS and GDPR), by including models that consider uncertainty and expert thoughts.
- *Multi-Layer Security Decision Support:* Developing hybrids of decision-support systems that apply CSV-NS logic to study security performance at the application, network, and hardware layers within financial organizations.
- *Theoretical Advancements:* The CSV-NS approach has been proposed for developing neutrosophic structures and bipolar frameworks to deal with both opposite risk results and tricky decision conditions.

Overall, the CSV-NS-based decision framework allows for stronger and more useful evaluations of encryption and decryption protocols in banking security. It points to a promising future for intelligent, safe, and uncertainty-driven decision systems used in both financial and cyber security areas.

Declaration of Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.
The authors also declare that there is no conflict of interests regarding the publication of this paper.

Data Availability: No data were used to support this study.
Conflict of interest: The authors declare that they have no conflict of interest.
Financial disclosure: The authors received no specific funding for this work.

References

1. Thabit, F., Can, O., Wani, R. U. Z., Qasem, M. A., Thorat, S. B., & Alkhzaimi, H. A. (2023). Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. Concurrency and Computation: Practice and Experience, 35(21), e7691.
2. Paar, C., Pelzl, J., & Güneysu, T. (2024). The advanced encryption standard (AES). In Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms (pp. 111-146). Berlin, Heidelberg: Springer Berlin Heidelberg.

3. BC, D. D., Banerjee, S., Pawar, K., & Murthy, A. V. R. (2025). Practical realization and performance analysis of Rivest-Shamir-Adleman encryption for secure underwater optical communication. Next Research, 2(2), 100225.
4. Sarkar, A. (2024). Recurrent neural networks-guided vector-valued synchronized key exchange for secure and privacy-preserving communication in Industrial Internet of Things. Applied Soft Computing, 161, 111731.
5. Gulen, U., & Baktir, S. (2023). Side-channel resistant 2048-bit RSA implementation for wireless sensor networks and internet of things. IEEE Access, 11, 39531-39543.
6. Sudharshan, R., Yogesh, P., & Prathiba, A. (2024, November). Enhancing AES Security and Performance: A Novel 8-bit Architecture with Unique Key Expansion for IoT Applications. In 2024 IEEE Silchar Subsection Conference (SILCON 2024) (pp. 1-6). IEEE.
7. Kamran, M., Ashraf, S., Salamat, N., Naeem, M., & Botmart, T. (2023). Cyber security control selection based decision support algorithm under single valued neutrosophic hesitant fuzzy Einstein aggregation information. Aims Mathematics, 8(3), 5551-5573.
8. Zadeh, L. A. (1965). Fuzzy sets. Information and control, 8(3), 338-353.
9. Atanassov, K. (1988). Review and new results on intuitionistic fuzzy sets. preprint IM-MFAIS-1-88, sofia, 5(1).
10. Smarandache, F. (2019). Neutrosophic set is a generalization of intuitionistic fuzzy set, inconsistent intuitionistic fuzzy set (picture fuzzy set, ternary fuzzy set), pythagorean fuzzy set, spherical fuzzy set, and q-rung orthopair fuzzy set, while neutrosophication is a generalization of regret theory, grey system theory, and three-ways decision (revisited). Journal of new theory, (29), 1-31.
11. Wang, H., Smarandache, F., Zhang, Y., & Sunderraman, R. (2010). Single valued neutrosophic sets. Infinite study.
12. Kamran, M., Salamat, N., Jana, C., & Xin, Q. (2025). Decision-making technique with neutrosophic Z-rough set approach for sustainable industry evaluation using sine trigonometric operators. Applied Soft Computing, 169, 112539.
13. Ye, J. (2013). Multicriteria decision-making method using the correlation coefficient under single-valued neutrosophic environment. International journal of general systems, 42(4), 386-394.
14. Peng, J. J., Wang, J. Q., Wang, J., Zhang, H. Y., & Chen, X. H. (2016). Simplified neutrosophic sets and their applications in multi-criteria group decision-making problems. International journal of systems science, 47(10), 2342-2358.
15. Mauri, L., & Damiani, E. (2022). Modeling threats to AI-ML systems using STRIDE. Sensors, 22(17), 6662.
16. Garg, H. (2020). Algorithms for single-valued neutrosophic decision making based on TOPSIS and clustering methods with new distance measure. Infinite Study.
17. Mondal, K., & Pramanik, S. (2014). Multi-criteria group decision making approach for teacher recruitment in higher education under simplified neutrosophic environment. Neutrosophic sets and Systems, 6, 28-34.
18. Kahraman, C., & Gündogdu, F. K. (2021). Decision making with spherical fuzzy sets. Studies in fuzziness and soft computing, 392, 3-25.
19. Karaaslan, M. F. (2021). A performance assessment of an HDG method for second-order Fredholm integro-differential equation: existence-uniqueness and approximation. Turkish Journal of Mathematics, 45(5), 2269-2281.
20. Kamran, M., Ashraf, S., Abdulla, M. E., & Fatima, S. (2025). Advancing Mathematical Frontiers: A Comprehensive Study of the Foundations of Fermatean Fuzzy Soft Linear Spaces and its Applications in Supply Chain Management. Information Sciences, 122506.
21. Nafei, A., Azizi, S. P., Edalatpanah, S. A., & Huang, C. Y. (2024). Smart TOPSIS: a neural Network-Driven TOPSIS with neutrosophic triplets for green Supplier selection in sustainable manufacturing. Expert systems with applications, 255, 124744.

22. Abdel-Basset, M., Gamal, A., Hezam, I. M., & Sallam, K. M. (2024). Sustainability assessment of optimal location of electric vehicle charge stations: a conceptual framework for green energy into smart cities. Environment, Development and Sustainability, 26(5), 11475-11513.
23. Klement, E. P., Mesiar, R., & Pap, E. (2013). Triangular norms (Vol. 8). Springer Science & Business Media.
24. Aczel, J., & Alsina, C. (1982). Characterizations of some classes of quasilinear functions with applications to triangular norms and to synthesizing judgements. Aequationes mathematicae, 25(1), 313-315.
25. Senapati, T. (2024). An Aczel-Alsina aggregation-based outranking method for multiple attribute decision-making using single-valued neutrosophic numbers. Complex & Intelligent Systems, 10(1), 1185-1199.
26. Liu, X. D., Chai, T. Y., & Wang, W. (2006). AFS fuzzy logic systems and its applications to model and control. International Journal of Information and Systems Sciences, 2(3), 285-305.
27. Atanassov, K. T., & Atanassov, K. T. (1999). Interval valued intuitionistic fuzzy sets (pp. 139-177). Physica-Verlag HD.
28. Farhadinia, B. (2013). Information measures for hesitant fuzzy sets and interval-valued hesitant fuzzy sets. Information Sciences, 240, 129-144.
29. Peng, X., & Yang, Y. (2015). Some results for Pythagorean fuzzy sets. International Journal of Intelligent Systems, 30(11), 1133-1160.
30. Akram, M., Shabir, M., c& Ashraf, A. (2021). Complex neutrosophic N-soft sets: A new model with applications. Neutrosophic Sets and Systems, 42(1), 18.

Received: July 28, 2025. Accepted: Jan 2, 2026