STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **16**, July 2026, pp 849–877.
Published online in International Academic Press (www.IAPress.org)

Structure-Preserving Clustering in Encrypted Feature Spaces

Haitham Qawaqneh [1], Wael Mahmoud Mohammed Salameh[2], Diana Amin Mohammad Mahmoud [3], Giorgio Nordo[4], Aqeedat Hussain[5], Arif Mehmood[5,*], Cris L. Armada[6,7]

[1]*Al-Zaytoonah University of Jordan, Amman 11733, Jordan*
[2]*Faculty of Information Technology, Abu Dhabi University, Abu Dhabi United Arab Emirates*
[3]*Amman Arab University, College of Arts and Sciences, Department of Mathematics, P.O. Box 2234, Amman 11953, Jordan*
[4]*MIFT Department of Mathematical and Computer Science, Physical Sciences and Earth Sciences - University of Messina, 98166 Sant' Agata, Messina, Italy*
[5]*Department of Mathematics, Institute of Numerical Sciences, Gomal University, Dera Ismail Khan 29050, KPK, Pakistan*
[6]*National University Ho Chi Minh City, Linh Trung Ward, Thu Duc City, Ho Chi Minh City, Vietnam*
[7]*Department of Applied Mathematics, Faculty of Applied Science, Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet, Ward 14, District 10, Ho Chi Minh City, Vietnam*

Abstract Complex single valued neutrosophic sets (CSVNSs) extend conventional neutrosophic sets to complex valued membership functions, providing a flexible mathematical model of uncertainty, indeterminacy, and inconsistency. Since each component of a universe is represented by truth, indeterminacy, and falsity membership functions with values in the unit interval, this enables the expression of richer and more expressive information in discrete and continuous models. Basic set-theoretic concepts of CSVNSs, such as subset hood, equality, union, intersection, complement, null set, and absolute set, are formally expressed and investigated. Information that exhibits phase-like or periodic behavior that can be described in the complex domain, in addition to being uncertain and incomplete, can be effectively represented by complex single valued neutrosophic sets (CSVNSs). In many real-world decision-making and pattern-recognition tasks, the evidence contains simultaneous degrees of truth, indeterminacy, and falsity. Additionally, classical similarity measures can become unstable when there is a preponderance of magnitude differences, scale dependence, and noise in the data. In order to assess the similarity between two CSVNS vectors, this study proposes a cotangent similarity assessment of Complex Single Valued Neutrosophic Sets (Cotangent CSVNS), which primarily relies on directional agreement and reduces the impact of raw distance. This study also presents privacy-sensitive clustering analysis using encrypted Iris data, both with and without feature normalization. Principal Component Analysis (PCA) is used to assess the quality of clustering using two-dimensional and three-dimensional visualization. While PCA is only used to map the encrypted representations to low-dimensional views summarizing the largest variance directions and making the cluster structure interpretable, Encrypted K-Means and Encrypted K-Means++ are used to identify three clusters on the encrypted feature space. The encrypted data does not eliminate the data's grouping tendencies, as evidenced by the two-dimensional PCA plots that show clusters that can be recognized as clearly distinguishable regions where the centroid values are well defined. Cluster boundaries are more balanced and smaller when normalization is performed before encryption since all feature magnitudes are scaled identically, increasing the reliability of distance separation. Additionally, the 3D PCA displays show that intra-cluster coherence and inter-cluster geometry are maintained by maintaining cluster separation in a more detailed reduced space with centroid separation and no group overlap. Centroid initialization, which selects spatially diverse starting points to improve convergence stability and reduce the likelihood of suboptimal partitions in encrypted applications, is improved by K-Means++. When the individual findings are combined, it is shown that unsupervised learning can be performed on encrypted and encrypted-normalized data while still producing meaningful structural patterns. This enables it to perform secure clustering, topology preservation, and analytics that respect privacy without revealing any underlying sensitive values.

Keywords Complex single-valued neutrosophic sets, Cotangent-based similarity measure, Privacy-preserving encrypted K-Means clustering, PCA-based visualization and topology preservation.

DOI: 10.19139/soic-2310-5070-3937

*Correspondence to: Arif Mehmood (Email: mehdaniyal@gmail.com). Department of Mathematics, Institute of Numerical Sciences, Gomal University, Dera Ismail Khan 29050, KPK, Pakistan.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

1. Introduction

In a world of information overload, distributed computation, and widespread uncertainty, classical mathematical and logical models tend to fail to reflect the complexity of the information in the real world. Incomplete data, conflicting evidence, change of preferences, and vague boundaries are not anomalies but are opportunities in fields as diverse as artificial intelligence and medical diagnosis, as well as in domains like secure multi-party computation, geopolitical risk analysis. A long-standing pressure has thus been towards generalized theories of uncertainty, which go beyond the bivalent truth paradigm. The most influential of these is the neutrosophic framework, which is a model which explicitly captures the indeterminacy as a separate element (not a derivative of truth or falsehood). This paradigm can be traced back to the work of Smarandache [1], who came up with neutrosophy as a new branch of philosophy, and consequently, neutrosophic logic, neutrosophic probability, and neutrosophic sets. This work, according to its abstract, unifies the logics, where all propositions can be defined by either truth value (T), or falsehood value (F), or indeterminacy value (I), all defined by subsets (which are a subset of) of the non-standard unit interval. The triadic structure enables the expression of paradox, contradiction and unknown in one formal system–a feature not available to either fuzzy logic or intuitionistic fuzzy logic. The early formulation, however, was based on non-standard analysis, which was difficult to compute. To solve this Wang et al. [2] suggested Single Valued Neutrosophic Sets (SVNS). Their abstract clearly mentions that SVNS limits the membership functions of truth, indeterminacy and falsity to standard unit interval [0,1], therefore, making practical applications in both engineering and computer science. Building on this, the same authors [3] came up with Interval Neutrosophic Sets (INS): membership degrees are defined as intervals (instead of a single number), and hence, a higher order uncertainty is taken into account regarding the membership values themselves. As highlighted in the abstract of [3], INS offer a more expressive and flexible format of handling incomplete or imprecise information, and can directly be applied to computing and multi criteria decision analysis. These theoretical constructs were practically manifested by a number of contributions to multi criteria decision making (MCDM). Zhang et al. [4] specifically considered interval neutrosophic sets and how to use them to solve MCDM problems. In their abstract, they describe a new score and accuracy function to compare interval neutrosophic numbers, and aggregation operators to allow the combination of subjective evaluations during group decision making. They show that their approach is superior to the intuitionistic fuzzy approaches when the indeterminacy is not negligible by providing case studies. Independently, Ye [5] investigated simplified neutrosophic sets (a superset of SVNS and INS) and had a family of aggregation operators, including the simplified neutrosophic weighted arithmetic average, to MCDM. The abstract of [5] underlines that these operators meet desirable characteristics such as idempotency and monotonicity, and are considered in a supplier selection problem, which demonstrates the universal character of neutrosophic information fusion. Another notable extension was made by Maji [6], who added the Neutrosophic Soft Set which is a combination of neutrosophic sets and soft set theory. According to its abstract, this hybrid model allows such reasoning with parameters under uncertainty, with each parameter being a neutrosophic set. This comes in handy especially when the criteria of decision themselves are themselves subject to vagueness or partial reliability as is the case in social sciences and medical diagnosis. Another route that Biswas et al. [7] explored through analysis incorporated the use of entropy and grey relational analysis during single valued neutrosophic evaluations. The abstract of [7] states that they first come up with an entropy measure used to objectively obtain the criterion weights using the neutrosophic decision matrix and then a grey relational coefficient, which measures the similarity between the alternatives and the ideal solutions. Their approach is confirmed on a green supplier selection problem, with a better discrimination power than non entropy methods. Applicability of neutrosophic sets is far more broadly applicable to symbolic decision tables into low level signal and image processing. Guo and Cheng [8] came up with a new neutrosophic method of image segmentation. They claim in their abstract that a picture is converted into the neutrosophic domain, with each pixel characterized by three categories: true (object), false (background), and indeterminate (edge or noise). Indeterminacy filter is applied next to eliminate the uncertainty and finally thresholding. The abstract performs better on medical images and natural images, particularly, where there is noise and low contrast. Based on this, Zhang, Zhang, and Cheng [9] combined neutrosophic logic with the watershed approach. The abstract of [9] points out that watershed transform tends to generate severe over segmentation owing to noise and local irregularities. The proposed method provides cleaner segmentation boundaries and

fewer spurious regions due to preprocessing the image with a neutrosophic filter that identifies and suppresses indeterminate regions. This paper also establishes neutrosophic sets as an effective front end to classical computer vision pipelines. To the strategic analysis, Pramanik and Roy [10] used neutrosophic game theory to determine the Indo Pak conflict over Jammu and Kashmir. Their abstract explains that traditional game theory does not work in circumstances in which the payoffs are indeterminate or where the parties have conflicting and incomplete information. They express the payoff of every player as neutrosophic numbers, thus not only model gains and losses, but also the level of uncertainty of the diplomatic, military, and economic outcomes. The neutrosophic equilibrium that follows offers more insights than the classical Nash equilibria and shows that neutrosophy can be used to inform conflict resolution and policy analysis in geopolitical environments with high stakes. Whereas neutrosophic models can address uncertainty in data and preferences, there has been a parallel revolution in the field of secure computation, the capability to do computations on encrypted data without ever having to decrypt it. This work of research commences with basic protocols.

1.1. Literature Review

The notion of secure multiparty computation and the so-called millionaire's problem which is a comparison of wealth between two parties without any numbers being disclosed was introduced by Yao [11]. The abstract of [11] outlines a generic way of generating and exchanging secrets in a secure manner, which forms the theoretical foundation of all further cryptographic protocols. Several decades later, Gentry [12] made a breakthrough and built the first homomorphic encryption (FHE) scheme. According to an abstract to his doctoral dissertation, FHE enables arbitrary computations on ciphertexts, and gives an encrypted result that, when decrypted, is identical to the result of the same operations on the plaintexts. This removed the trust requirement to the computing party, making computation on sensitive information to be outsourced. Bost et al. [13] connected cryptography and machine learning by showing machine learning classification on encrypted data. Their abstract provides an overview of how to assess decision trees, naive Bayes, and support vector machines when using FHE or a homomorphic encryption that is somewhat homomorphic, so that a cloud server can classify medical records or financial records without ever having seen the underlying data. It is more specifically applicable to neutrosophic decision systems: when the input data are indeterminate the same level of uncertainty should be maintained and be processed homomorphically. This was subsequently considered by Jaschke and Armknecht [14], who suggested accelerating homomorphic computations in machine learning by employing optimizations to make the multiplicative depth and computational overhead smaller. The abstract focuses on practicality, delivering important speedups to encrypted neural network layers. Patel et al. [15] conducted a literature review on privacy preserving data mining with homomorphic encryption, and systematically compared various schemes of the HE (Paillier, BGV, CKKS) and how they can be applied to data clustering, association rule mining, and classification. The abstract of [15] concludes that although FHE is still a computationally intensive approach, new developments render it to be feasible on small to medium-sized datasets and, in particular, on use cases like healthcare analytics. In addition to classification, encrypted data is particularly challenging to learn unsupervised. Arthur and Vassilvitskii [16] proposed k means++, a seeding algorithm that ensures that the k means objective has a better approximation bound. Their abstract mathematically demonstrates that the careful initialisation lessens the probability of bad clustering, which holds even when homomorphically computed distances are taken. The seeding step has to be rewritten in an encrypted environment to be used without exposing the cluster centroids or the point assignments. Privacy-preserving set intersection (PSI) and speedy database joins are a more general primitive of secure data processing. Mohassel et al. [17] suggest effective secret shared data protocols. The abstract explains how their procedures derive linear complexity of communication and malicious security, enabling two parties to perform the intersection of their datasets or more general equi joins and obtain the outcome without disclosing a non-intersecting element. These primitives are necessary when using neutrosophic computations made by many privacies sensitive outputs- e.g. many hospitals calculating a concerted neutrosophic choice without revealing patient records. At the same time, there is a more mathematical basis, which is essential in the study of the stability and convergence of neutrosophic operators, that has been established in operator theory. The correlation function of a class of non-stationary fields with a zero spectrum was studied by Hatamleh [18] who derived explicit forms which generalize classical Wiener Khinchin results. The abstract of [18] suggests signal processing implications and stochastic modeling implications,

especially when fields are long range dependent or spectral singularities-phenomena that can be re-conceived as a manifestation of indeterminacy. This was then generalized by Hatamleh and Zolotarev [19] to a two-dimensional model representation of commuting operators. Their abstract indicates that the pair of commuting operators with specified spectral properties may be modeled as multiplication operators on a space of vector valued functional, similar to the Sz. NagyFoias model. This expression gives a canonical form to study neutrosophic aggregation operators which do not necessarily need to be self-adjoint. The same authors [20] also took into account the case of non selfadjoint operators whose imaginary component is of infinitely dimensional dimension, and they built model representations that are a separation of the self-adjoint and dissipative terms. The abstract of [20] outlines the applications to scattering theory and non-stationary processes, where the imaginary component represents the loss of energy or information decayconceptually the same as the growing indeterminacy with time. Elaborating this theme, Hatamleh and Zolotarev [21] constructed triangular models of commutative systems of linear operators near to unitary operators. The abstract of [21] shows that any commuting family of operators that has a unitary dilation may be expressed as a triangular matrix of multiplication operators, extending the classical Jordan form to an infinite-dimensional version. These triangular shapes are directly applicable to simplification of neutrosophic MCDM operators, so that complex decision rules can be broken down into more straightforward, easier to analyze steps. The latest are explicitly connected with the neutrosophic tradition and the current topological and plithogenic constructions. Hatamleh and Hazaymeh [22] research the topological space on the basis of symbolic n plithogenic intervals. Their abstract explains that plithogenic sets are generalizations of neutrosophic ones, that they permit any number of attributes (not necessarily truth, indeterminacy, falsehood) and that they include a certain level of contradiction between their attributes. Symbolic n plithogenic intervals are intervals on the real line which have symbolic labels that denote various refinements of attributes. The authors develop a topology on such intervals, explore its separation axioms, compactness and connectedness, and demonstrate that classical neutrosophic topologies are special cases. This work gives the mathematical framework of the construction of continuous, well-behaved operations on plithogenic data. In this, Qawasmeh and Hatamleh [23] suggested a new contraction constructed on H simulation functions in extended b metric spaces, and applied it to integral equations. It is mentioned in the abstract that the unification of many well-known contraction conditions is achieved by the H simulation functions (Banach, Kannan, Chatterjee). They establish fixed point theorems of these contractions in extended b metric spaces, in which the triangle inequality is weakened by a multiplicative constant. These fixed-point solutions are important to ensure convergence of iterative algorithms to neutrosophic aggregation, entropy minimization, and homomorphically encrypted iterative computations (e.g., encrypted gradient descent). Lastly, Heilat et al. [24] introduced a new spline technique in solving any two-point linear problems with a boundary value problem. The abstract of [24] outlines the construction of cubic and quintic splines which satisfy the differential equation at collocation points and have a higher order convergence than standard finite difference methods. Although it largely appears unrelated to neutrosophic logic, spline approximations are needed whenever a continuous interpretation of discrete neutrosophic data is needed such as during interpolation of membership functions or when building approximate homomorphic functions over real numbers.

The last few years have seen an unprecedented advance in the theory of fixed point theory, fractional calculus and their various applications in applied mathematics and computational sciences. The role fixed point theory in particular plays in nonlinear analysis is that it is useful in answering the question of existence and uniqueness of solutions to various classes of equations. In this direction, H. Qawaghneh [26] formulated fractional analytic solutions with fixed point methods, which give powerful solutions to complex mathematical models occurring in applied situations. More steps have been developed by generalizing the fixed point results to generalized metric structures. As an illustration, H. Qawaghneh et al. [27] explored the fixed point results in partial b-metric space, which is a more flexible framework of modeling non-standard distance functions. In the same manner, H. Qawaqneh et al. [28] proposed new characterizations of fuzzy contractions in fuzzy b-metric spaces that play a significant role in the processing of uncertainty and vagueness in mathematical modelling. Besides these theoretical advances, there are recent papers that address the usage of fractional calculus in physical modeling. H. Qawaqneh et al. [29] studied stability, modulation instability and fractional soliton solutions of Van der Waals equation, proving the power of fractional methods in describing nonlinear physical phenomena. Also, H. Qawaqneh [30] introduced new functions of fixed point results in metric spaces and H. Qawaqneh et al. [31] proposed new

geometric contraction mappings of fractional metric spaces which enhanced the theoretical basis of the field.
At the applied level, the modern methods of computations have greatly expanded the horizons of these mathematical systems. As an example, M. Elbes et al. [32]created a deep learning-based COVID-19 detection system based on the use of X-ray images, which can be interpreted as an indication of the practical significance of advanced mathematical and computational tools. Similarly, T. Kanan et al. [33] examined learning environments that were based on IoT, noting that intelligent systems were integrated into the learning environment.
In general, all these contributions demonstrate a great interplay between the theoretical developments and the practical application that prove the significance of fixed point theory, fuzzy systems, and the use of the fractional analysis in solving the current scientific challenges.

1.2. Research Questions

1. What do Complex Single-Valued Neutrosophic Sets (CSVNSs) offer in terms of improved representation of uncertainty, indeterminacy and inconsistency, as opposed to classical neutrosophic sets?
2. How can the complex-valued membership functions of CSVNSs be used to model phase or periodic phenomena in uncertain and incomplete information?
3. How can basic set operations (subset, equality, union, intersection, complement, null set, and absolute set) be defined and studied in the setting of CSVNSs?
4. What are the challenges faced by traditional similarity measures when used with CSVNS data, especially in cases where magnitudes, scales, and noise are present?
5. What are the benefits of the proposed cotangent-based similarity measure (Cotangent CSVNS) in assessing similarity based on direction rather than distance? 6. Does privacy-preserving clustering on encrypted data, like the Iris dataset, preserve the data's structure?
7. How does data normalization before encryption affect the clustering, cluster compactness and inter-cluster separation?
8. To what extent can Principal Component Analysis (PCA) be used to interpret and represent clustering results in encrypted data using two-dimensional and three-dimensional projections?
9. What are the performance of Encrypted K-Means and Encrypted K-Means++ in discovering clusters in encrypted feature spaces?
10. How does K-Means++ initialization enhance stability and prevent suboptimal clustering in encrypted data?
11. How well are cluster compactness and cluster separation maintained in encrypted and normalized encrypted data?
12. Is the proposed framework capable of secure clustering and topology preservation, while enabling secure and privacy-preserving analytics without compromising valuable data?

1.3. Novelty

Privacy-preserving end-to-end clustering pipeline that protects privacy by running K-Means and K-Means++ on encrypted Iris data, demonstrating that unsupervised learning is still feasible without revealing raw features. Normalization-before-encryption comparison shows how feature scale affects the consistency of distance-based clustering under encryption by explicitly comparing encrypted data before and after a pre-processing stage of normalization. Cluster separability, centroid spacing, and geometric structure maintenance of encrypted representations are demonstrated, and multi-view structure is validated using two-dimensional and three-dimensional PCA representations of encrypted representations with interpretive only. Even in an intermediate feature space with protection, the encrypted K-Means++ contribution shows that informed centroid initialization improves convergence stability and minimizes the occurrence of suboptimal local minima. Evidence of topology and geometry preservation provides centroid-based and visual proof that encryption may maintain intra-cluster compactness and inter-cluster separation, which in turn supports the effective implementation of privacy-compliant analytics.

2. Preliminaries

In this section, we will give some preliminary information for the present study.

Definition 2.1
[1] Let $\mathcal{U}$ be an universe of discourse. Then the neutrosophic set P can be presented of the form:

$$\mathrm{P} = \{\langle \mathbf{x}, \mathrm{T}_P(\mathbf{x}), \mathrm{I}_P(\mathbf{x}), \mathrm{F}_P(\mathbf{x})\rangle : \mathbf{x} \in \mathcal{U}\}$$

where the function $\mathrm{T}, \mathrm{I}, \mathrm{F} : U \longrightarrow]^{-}0, 1^{+}[$ defines respectively the degree of membership, the degree of indeterminacy, and the degree of non-membership of the element $\mathbf{x} \in \mathcal{U}$ to the set P satisfying the following condition.

$$^{-}0 \leq sup\mathrm{T}_P(\mathbf{x}) + sup\mathrm{I}_P(\mathbf{x}) + sup\mathrm{F}_P(\mathbf{x}) \leq 3^{+}$$

From philosophical point of view, the neutrosophic set assumes the value from real standard or non-standard subsets of $]^{-}0, 1^{+}[$. So instead of $]^{-}0, 1^{+}[$ needs to take the interval $[0, 1]$ for technical applications, because $]^{-}0, 1^{+}[$ will be difficult to apply in the real applications such as scientific and engineering problems.

Definition 2.2
[1]Let there be two neutrosophic sets (NSs),

$$P_{NS} = \{\langle \mathbf{x}, \mathrm{T}_P(\mathbf{x}), \mathrm{I}_P(\mathbf{x}), \mathrm{F}_P(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

and

$$Q_{NS} = \{\langle \mathbf{x}, \mathrm{T}_Q(\mathbf{x}), \mathrm{I}_Q(\mathbf{x}), \mathrm{F}_Q(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

then $P_{NS} \subseteq Q_{NS}$ iff $\mathrm{T}_P(\mathbf{x}) \leq \mathrm{T}_Q(\mathbf{x}), \mathrm{I}_P(\mathbf{x}) \geq \mathrm{I}_Q(\mathbf{x}), \mathrm{F}_P(\mathbf{x}) \geq \mathrm{F}_Q(\mathbf{x})$.

Definition 2.3
[1]Let there be two neutrosophic sets (NSs),

$$P_{NS} = \{\langle \mathbf{x}, \mathrm{T}_P(\mathbf{x}), \mathrm{I}_P(\mathbf{x}), \mathrm{F}_P(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

and

$$Q_{NS} = \{\langle \mathbf{x}, \mathrm{T}_Q(\mathbf{x}), \mathrm{I}_Q(\mathbf{x}), \mathrm{F}_Q(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

then $P_{NS} = Q_{NS}$ iff $\mathrm{T}_P(\mathbf{x}) = \mathrm{T}_Q(\mathbf{x}), \mathrm{I}_P(\mathbf{x}) = \mathrm{I}_Q(\mathbf{x}), \mathrm{F}_P(\mathbf{x}) = \mathrm{F}_Q(\mathbf{x})$.

Definition 2.4
[2]Let $\mathbb{X}$ be a space of points (objects) with generic elements in $\mathbb{X}$ denoted by $\mathbf{x}$. A Single-Valued Neutrosophic set (SVNS) $\mathcal{A}$ in $\mathbb{X}$ is characterized by truth membership function $\mathrm{T}_{\mathcal{A}}\mathbf{x}$, indeterminacy membership function $\mathrm{I}_{\mathcal{A}}\mathbf{x}$, and falsity membership function $\mathrm{F}_{\mathcal{A}}\mathbf{x}$. For each point $\mathbf{x} \in \mathbb{X}$, there are $\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{A}}\mathbf{x} \in [0, 1]$ and $0 \leq \mathrm{T}_{\mathcal{A}}\mathbf{x} + \mathrm{I}_{\mathcal{A}}\mathbf{x} + \mathrm{F}_{\mathcal{A}}\mathbf{x} \leq 3$. Therefore, an SVNS $\mathcal{A}$ can be represented by

$$\mathcal{A} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{A}}\mathbf{x}\rangle | \mathbf{x} \in \mathbb{X}\}.$$

Definition 2.5
[2]Let $\mathcal{A}$ be an SVNS over $\mathbb{X}$. Then complement of $\mathcal{A}$ is denoted by $\mathcal{A}^c$ and is defined as;

$$\mathcal{A}^c = \{\langle \mathbf{x}, \mathrm{F}_{\mathcal{A}}\mathbf{x}, 1 - \mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{A}}\mathbf{x}\rangle | \mathbf{x} \in \mathbb{X}\}$$

3. Characterization of Complex Single Valued Neutrosophic Sets

Definition 3.1
[25] A complex neutrosophic set S defined on a universe of discourse $\mathbb{X}$ is characterized by a truth membership

function $\mathrm{T}_S(\mathbf{x})$, an indeterminacy membership function $\mathrm{I}_S(\mathbf{x})$, and a falsity membership function $\mathrm{F}_S(\mathbf{x})$, assigning complex-valued grades to each $\mathbf{x} \in \mathbb{X}$. The values $\mathrm{T}_S(\mathbf{x})$, $\mathrm{I}_S(\mathbf{x})$, $\mathrm{F}_S(\mathbf{x})$ and their sum lie within the unit circle in the complex plane and are given by

$$\mathrm{T}_S(\mathbf{x}) = p_S(\mathbf{x})e^{j\mu_S(\mathbf{x})}, \quad \mathrm{I}_S(\mathbf{x}) = q_S(\mathbf{x})e^{j\nu_S(\mathbf{x})}, \quad \mathrm{F}_S(\mathbf{x}) = r_S(\mathbf{x})e^{j\omega_S(\mathbf{x})},$$

where $p_S(\mathbf{x}), q_S(\mathbf{x}), r_S(\mathbf{x}) \in [0,1]$ and $\mu_S(\mathbf{x}), \nu_S(\mathbf{x}), \omega_S(\mathbf{x})$ are real-valued functions such that

$$0 \leq p_S(\mathbf{x}) + q_S(\mathbf{x}) + r_S(\mathbf{x}) \leq 3.$$

The complex neutrosophic set S can be represented as

$$S = \{\langle \mathbf{x}, \mathrm{T}_S(\mathbf{x}), \mathrm{I}_S(\mathbf{x}), \mathrm{F}_S(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\},$$

where

$$\mathrm{T}_S : \mathbb{X} \to \{a_{\mathrm{T}} \in \mathbb{C} : |a_{\mathrm{T}}| \leq 1\}, \quad \mathrm{I}_S : \mathbb{X} \to \{a_{\mathrm{I}} \in \mathbb{C} : |a_{\mathrm{I}}| \leq 1\},$$
$$\mathrm{F}_S : \mathbb{X} \to \{a_{\mathrm{F}} \in \mathbb{C} : |a_{\mathrm{F}}| \leq 1\},$$

and

$$|\mathrm{T}_S(\mathbf{x})| + |\mathrm{I}_S(\mathbf{x})| + |\mathrm{F}_S(\mathbf{x})| \leq 3.$$

The interval $(0, 2\pi]$ is chosen for the phase term to be in line with the original definition of a complex fuzzy set in which the amplitude terms lie in an interval of $(0,1)$, and the phase terms lie in an interval of $(0, 2\pi]$.
Throughout the paper, a complex neutrosophic set refers to a neutrosophic set with complex-valued truth, indeterminacy, and falsity membership functions, while the classical neutrosophic set refers to the case where these membership functions are real-valued.

Remark 3.1
In the definition above, ι denotes the imaginary number $\iota = \sqrt{-1}$ and it is this imaginary number ι that makes the CNS have complex-valued membership grades. The term $e^{\iota\theta}$ denotes the exponential form of a complex number and represents $e^{\iota\theta} = \cos\theta + \iota\sin\theta$.

Definition 3.2
Let there be two complex single valued neutrosophic sets (CSVNSs),

$$\mathcal{A}_{CSVNS} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{A}}(\mathbf{x}), \mathrm{I}_{\mathcal{A}}(\mathbf{x}), \mathrm{F}_{\mathcal{A}}(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

and

$$\mathcal{B}_{CSVNS} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{B}}(\mathbf{x}), \mathrm{I}_{\mathcal{B}}(\mathbf{x}), \mathrm{F}_{\mathcal{B}}(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

then $\mathcal{A}_{CSVNS} \subseteq \mathcal{B}_{CSVNS}$ iff $\mathrm{T}_{\mathcal{A}}(\mathbf{x}) \leq \mathrm{T}_{\mathcal{B}}(\mathbf{x}), \mathrm{I}_{\mathcal{A}}(\mathbf{x}) \geq \mathrm{I}_{\mathcal{B}}(\mathbf{x}), \mathrm{F}_{\mathcal{A}}(\mathbf{x}) \geq \mathrm{F}_{\mathcal{B}}(\mathbf{x})$.

Definition 3.3
Let there be complex single valued neutrosophic sets (CSVNSs),

$$\mathcal{A}_{CSVNS} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{A}}(\mathbf{x}), \mathrm{I}_{\mathcal{A}}(\mathbf{x}), \mathrm{F}_{\mathcal{A}}(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

and

$$\mathcal{B}_{CSVNS} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{B}}(\mathbf{x}), \mathrm{I}_{\mathcal{B}}(\mathbf{x}), \mathrm{F}_{\mathcal{B}}(\mathbf{x})\rangle : \mathbf{x} \in \mathbb{X}\}$$

then $\mathcal{A}_{CSVNS} = \mathcal{B}_{CSVNS}$ iff $\mathrm{T}_{\mathcal{A}}(\mathbf{x}) = \mathrm{T}_{\mathcal{B}}(\mathbf{x}), \mathrm{I}_{\mathcal{A}}(\mathbf{x}) = \mathrm{I}_{\mathcal{B}}(\mathbf{x}), \mathrm{F}_{\mathcal{A}}(\mathbf{x}) = \mathrm{F}_{\mathcal{B}}(\mathbf{x})$.

Definition 3.4
Let $\mathcal{A}$ and $\mathcal{B}$ be two complex single-valued neutrosophic sets over the universe set $\mathbb{X}$. Then their union is represented by $\mathcal{A} \cup \mathcal{B} = \mathcal{C}$ is defined by:

$$\mathcal{C} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{C}}\mathbf{x}, \mathrm{I}_{\mathcal{C}}\mathbf{x}, \mathrm{F}_{\mathcal{C}}\mathbf{x}\rangle : \mathbf{x} \in \mathbb{X}\},$$

Where

$$\mathrm{T}_{\mathcal{C}}\mathbf{x} = \max\{\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\}$$
$$\mathrm{I}_{\mathcal{C}}\mathbf{x} = \max\{\mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{B}}\mathbf{x}\}$$
$$\mathrm{F}_{\mathcal{C}}\mathbf{x} = \min\{\mathrm{F}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\}$$

Definition 3.5
Let $\mathcal{A}$ and $\mathcal{B}$ be two complex single-valued neutrosophic sets over the universe set $\mathbb{X}$. Then their intersection is represented by $\mathcal{A} \cap \mathcal{B} = \mathcal{C}$ is defined by:

$$\mathcal{C} = \{\langle \mathbf{x}, \mathrm{T}_{\mathcal{C}}\mathbf{x}, \mathrm{I}_{\mathcal{C}}\mathbf{x}, \mathrm{F}_{\mathcal{C}}\mathbf{x}\rangle : \mathbf{x} \in \mathbb{X}\},$$

Where

$$\mathrm{T}_{\mathcal{C}}\mathbf{x} = \min\{\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\}$$
$$\mathrm{I}_{\mathcal{C}}\mathbf{x} = \min\{\mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{B}}\mathbf{x}\}$$
$$\mathrm{F}_{\mathcal{C}}\mathbf{x} = \max\{\mathrm{F}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\}$$

Definition 3.6
Let $\{\mathcal{A}_i : i \in I\}$ be a family of complex single-valued neutrosophic sets over the universe set $\mathbb{X}$. Then,

$$\bigcup_{i\in I}\mathcal{A}_i = \left\{\langle \mathbf{x}, \sup_{i\in I}\mathrm{T}_{\mathcal{A}_i}\mathbf{x}, \sup_{i\in I}\mathrm{I}_{\mathcal{A}_i}\mathbf{x}, \inf_{i\in I}\mathrm{F}_{\mathcal{A}_i}\mathbf{x}\rangle : \mathbf{x} \in \mathbb{X}\right\}.$$

$$\bigcap_{i\in I}\mathcal{A}_i = \left\{\langle \mathbf{x}, \inf_{i\in I}\mathrm{T}_{\mathcal{A}_i}\mathbf{x}, \inf_{i\in I}\mathrm{I}_{\mathcal{A}_i}\mathbf{x}, \sup_{i\in I}\mathrm{F}_{\mathcal{A}_i}()\rangle : \mathbf{x} \in \mathbb{X}\right\}.$$

Definition 3.7
A complex single-valued neutrosophic set $\mathcal{A}$ over the universe set $\mathbb{X}$ is said to be a *null complex single-valued neutrosophic set* if

$$\mathrm{T}_{\mathcal{A}}\mathbf{x} = 0, \quad \mathrm{I}_{\mathcal{A}}\mathbf{x} = 0, \quad \mathrm{F}_{\mathcal{A}}\mathbf{x} = 1, \quad \forall\, \mathbf{x} \in \mathbb{X}.$$

It is denoted by $0_{\mathcal{A}}$.

Definition 3.8
A complex single-valued neutrosophic set $\mathcal{A}$ over the universe set $\mathbb{X}$ is said to be a *absolute complex single-valued neutrosophic set* if

$$\mathrm{T}_{\mathcal{A}}\mathbf{x} = 1, \quad \mathrm{I}_{\mathcal{A}}\mathbf{x} = 1, \quad \mathrm{F}_{\mathcal{A}}\mathbf{x} = 0, \quad \forall\, \mathbf{x} \in \mathbb{X},$$

Clearly,

$$0^c_{\mathcal{A}} = 1_{\mathcal{A}}, \quad 1^c_{\mathcal{A}} = 0_{\mathcal{A}}.$$

Proposition 1
Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be three complex single-valued neutrosophic sets over the universe set $\mathbb{X}$. Then,

1. $\mathcal{A} \cup [\mathcal{B} \cup \mathcal{C}] = [\mathcal{A} \cup \mathcal{B}] \cup \mathcal{C} and$
   $\mathcal{A} \cap [\mathcal{B} \cap \mathcal{C}] = [\mathcal{A} \cap \mathcal{B}] \cap \mathcal{C}$;
2. $\mathcal{A} \cup [\mathcal{B} \cap \mathcal{C}] = [\mathcal{A} \cup \mathcal{B}] \cap [\mathcal{A} \cup \mathcal{C}] and$
   $\mathcal{A} \cap [\mathcal{B} \cup \mathcal{C}] = [\mathcal{A} \cap \mathcal{B}] \cup [\mathcal{A} \cap \mathcal{C}]$;
3. $\mathcal{A} \cup 0_{\mathcal{A}} = \mathcal{A} and \mathcal{A} \cap 0_{\mathcal{A}} = 0_{\mathcal{A}}$;
4. $\mathcal{A} \cup 1_{\mathcal{A}} = \mathcal{A} and \mathcal{A} \cap 1_{\mathcal{A}} = \mathcal{A}$;

Proof
Obvious. □

Proposition 2
Let $\mathcal{A}$ and $\mathcal{B}$ be two complex single-valued neutrosophic sets over the universe set $\mathbb{X}$. Then,

1. $[\mathcal{A} \cup \mathcal{B}]^c = \mathcal{A}^c \cap \mathcal{B}^c$

2. $[\mathcal{A} \cap \mathcal{B}]^c = \mathcal{A}^c \cup \mathcal{B}^c$

Proof
(i). For all and $\mathbf{x} \in \mathbb{X}$,

$$\begin{aligned}\mathcal{A} \cup \mathcal{B} = \{\langle \mathbf{x}, \max\{\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\}, \max\{\mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{B}}\mathbf{x}\},\\ \min\{\mathrm{F}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\}\rangle\}\\ [\mathcal{A} \cup \mathcal{B}]^c = \{\langle \mathbf{x}, \min\{\mathrm{F}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\}, 1 - \max\{\mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{B}}\mathbf{x}\},\\ \max\{\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\}\rangle\}\end{aligned}$$

Now,

$$\begin{aligned}\mathcal{A}^c = \{\langle \mathbf{x}, \mathrm{F}_{\mathcal{A}}\mathbf{x}, 1 - \mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{A}}\mathbf{x}\rangle\}\\ \mathcal{B}^c = \{\langle \mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}, 1 - \mathrm{I}_{\mathcal{B}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\rangle\}\end{aligned}$$

Then,

$$\begin{aligned}\mathcal{A}^c \cap \mathcal{B}^c &= \{\langle \mathbf{x}, \min\{\mathrm{F}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\}, \min\{1 - \mathrm{I}_{\mathcal{A}}\mathbf{x}, 1 - \mathrm{I}_{\mathcal{B}}\mathbf{x}\},\\ &\quad \max\{\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\}\rangle\}\\ &= \{\langle \mathbf{x}, \min\{\mathrm{F}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\}, 1 - \max\{\mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{B}}\mathbf{x}\},\\ &\quad \max\{\mathrm{T}_{\mathcal{A}}\mathbf{x}, \mathrm{T}_{\mathcal{B}}\mathbf{x}\}\rangle\}\end{aligned}$$

Therefore, $[\mathcal{A} \cup \mathcal{B}]^c = \mathcal{A}^c \cap \mathcal{B}^c$.
(ii). It is obtained in a similar way. □

Example 3.1
Suppose that, the universe set $\mathbb{X}$ given by $\mathbb{X} = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$. Let us consider complex single-valued neutrosophic sets $\mathcal{A}\, and\, \mathcal{B}$ over the universe set $\mathbb{X}$ as follows

$$\mathcal{A} = \begin{bmatrix}(\langle x_1, 0.3e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.3)}, 0.6e^{\iota\pi(0.5)}\rangle, \langle x_2, 0.4e^{\iota\pi(0.3)}, 0.2e^{\iota\pi(0.1)}, 0.8e^{\iota\pi(0.7)}\rangle,\\ \langle x_3, 0.6e^{\iota\pi(0.5)}, 0.2e^{\iota\pi(0.1)}, 0.5e^{\iota\pi(0.4)}\rangle, \langle x_4, 0.2e^{\iota\pi(0.1)}, 0.3e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.3)}\rangle)\\ (\langle x_1, 0.4e^{\iota\pi(0.3)}, 0.3e^{\iota\pi(0.2)}, 0.8e^{\iota\pi(0.7)}\rangle, \langle x_2, 0.3e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.3)}, 0.2e^{\iota\pi(0.1)}\rangle,\\ \langle x_3, 0.3e^{\iota\pi(0.2)}, 0.2e^{\iota\pi(0.1)}, 0.7e^{\iota\pi(0.6)}\rangle, \langle x_4, 0.1e^{\iota\pi(0.1)}, 0.2e^{\iota\pi(0.1)}, 0.9e^{\iota\pi(0.8)}\rangle)\end{bmatrix}$$

$$\mathcal{B} = \begin{bmatrix}(\langle x_1, 0.6e^{\iota\pi(0.5)}, 0.3e^{\iota\pi(0.2)}, 0.8e^{\iota\pi(0.7)}\rangle, \langle x_2, 0.2e^{\iota\pi(0.1)}, 0.5e^{\iota\pi(0.4)}, 0.8e^{\iota\pi(0.7)}\rangle,\\ \langle x_3, 0.1e^{\iota\pi(0.1)}, 0.1e^{\iota\pi(0.1)}, 0.4e^{\iota\pi(0.3)}\rangle, \langle x_4, 0.5e^{\iota\pi(0.4)}, 0.2e^{\iota\pi(0.1)}, 0.3e^{\iota\pi(0.2)}\rangle)\\ (\langle x_1, 0.7e^{\iota\pi(0.6)}, 0.5e^{\iota\pi(0.4)}, 0.6e^{\iota\pi(0.5)}\rangle, \langle x_2, 0.4e^{\iota\pi(0.3)}, 0.2e^{\iota\pi(0.1)}, 0.3e^{\iota\pi(0.2)}\rangle,\\ \langle x_3, 0.5e^{\iota\pi(0.4)}, 0.3e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.3)}\rangle, \langle x_4, 0.4e^{\iota\pi(0.3)}, 0.2e^{\iota\pi(0.1)}, 0.6e^{\iota\pi(0.5)}\rangle)\end{bmatrix}$$

Then, their union and intersection operations are given as follows:

$$\mathcal{A} \cup \mathcal{B} = \begin{bmatrix}(\langle x_1, 0.6e^{\iota\pi(0.5)}, 0.4e^{\iota\pi(0.3)}, 0.6e^{\iota\pi(0.5)}\rangle, \langle x_2, 0.4e^{\iota\pi(0.3)}, 0.5e^{\iota\pi(0.4)}, 0.8e^{\iota\pi(0.7)}\rangle,\\ \langle x_3, 0.6e^{\iota\pi(0.5)}, 0.2e^{\iota\pi(0.1)}, 0.4e^{\iota\pi(0.3)}\rangle, \langle x_4, 0.5e^{\iota\pi(0.4)}, 0.3e^{\iota\pi(0.2)}, 0.3e^{\iota\pi(0.2)}\rangle)\\ (\langle x_1, 0.7e^{\iota\pi(0.6)}, 0.5e^{\iota\pi(0.4)}, 0.6e^{\iota\pi(0.5)}\rangle, \langle x_2, 0.4e^{\iota\pi(0.3)}, 0.4e^{\iota\pi(0.3)}, 0.2e^{\iota\pi(0.1)}\rangle,\\ \langle x_3, 0.5e^{\iota\pi(0.4)}, 0.3e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.3)}\rangle, \langle x_4, 0.4e^{\iota\pi(0.3)}, 0.2e^{\iota\pi(0.1)}, 0.6e^{\iota\pi(0.5)}\rangle)\end{bmatrix}$$

$$\mathcal{A} \cap \mathcal{B} = \begin{bmatrix}(\langle x_1, 0.3e^{\iota\pi(0.2)}, 0.3e^{\iota\pi(0.3)}, 0.8e^{\iota\pi(0.7)}\rangle, \langle x_2, 0.2e^{\iota\pi(0.1)}, 0.2e^{\iota\pi(0.1)}, 0.8e^{\iota\pi(0.7)}\rangle,\\ \langle x_3, 0.1e^{\iota\pi(0.1)}, 0.1e^{\iota\pi(0.1)}, 0.5e^{\iota\pi(0.4)}\rangle, \langle x_4, 0.2e^{\iota\pi(0.1)}, 0.2e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.4)}\rangle)\\ (\langle x_1, 0.3e^{\iota\pi(0.2)}, 0.3e^{\iota\pi(0.3)}, 0.8e^{\iota\pi(0.7)}\rangle, \langle x_2, 0.2e^{\iota\pi(0.1)}, 0.2e^{\iota\pi(0.1)}, 0.8e^{\iota\pi(0.7)}\rangle,\\ \langle x_3, 0.1e^{\iota\pi(0.1)}, 0.1e^{\iota\pi(0.1)}, 0.5e^{\iota\pi(0.4)}\rangle, \langle x_4, 0.2e^{\iota\pi(0.1)}, 0.2e^{\iota\pi(0.2)}, 0.4e^{\iota\pi(0.3)}\rangle)\end{bmatrix}$$

4. Cotangent Similarity Measures for Complex Single Valued Neutrosophic Sets

Let $\mathcal{A} = \langle \mathbf{x}, \mathbf{T}_{\mathcal{A}}\mathbf{x}, \mathrm{I}_{\mathcal{A}}\mathbf{x}, \mathrm{F}_{\mathcal{A}}\mathbf{x}\rangle$ and $\mathcal{B} = \langle \mathbf{x}, T_{\mathcal{B}}\mathbf{x}, \mathrm{I}_{\mathcal{B}}\mathbf{x}, \mathrm{F}_{\mathcal{B}}\mathbf{x}\rangle$ be two Complex single valued neutrosophic numbers. Now cotangent similarity function which measures the similarity between two vectors based only on the direction, ignoring the impact of the distance between them can be presented as follows:

$$Cotangent_{CSVNS}(\mathcal{A},\mathcal{B}) = \frac{1}{n}\sum_{k=1}^{n}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|T_{ik} - T_{jk}| + |I_{ik} - I_{jk}| + |F_{ik} - F_{jk}|)]\}$$

Proposition 3
The defined cotangent similarity measure $Cot_{CSVNS}(\mathcal{A},\mathcal{B})$ between $\mathcal{A}$ and $\mathcal{B}$ satisfies the following properties:

1. $0 \leq Cot_{CSVNS}(\mathcal{A},\mathcal{B}) \leq 1$.
2. $Cot_{CSVNS}(\mathcal{A},\mathcal{B}) = 1$ iff $\mathcal{A} = \mathcal{B}$.
3. $Cot_{CSVNS}(\mathcal{A},\mathcal{B}) = Cot_{CNRS}(\mathcal{B},\mathcal{A})$.
4. If R is a CSVNS in $\mathbb{X}$ and $\mathcal{A} \subset \mathcal{B} \subset \mathcal{C}$ then $Cot_{CSVNS}(\mathcal{A},\mathcal{C}) \leq Cot_{CSVNS}(\mathcal{A},\mathcal{B})$ and $Cot_{CSVNS}(\mathcal{A},\mathcal{C}) \leq Cot_{CSVNS}(\mathcal{B},\mathcal{C})$.

Proof

1. As the membership, indeterminacy and non-membership functions of the CSVNSs and the value of the cotangent function are within $[0,1]$, the similarity measure based on cotangent function also is within $[0,1]$. Hence $0 \leq Cot_{CSVNS}(\mathcal{A},\mathcal{B}) \leq 1$.
2. For any two CSVNS $\mathcal{A}$ and $\mathcal{B}$ if $\mathcal{A} = \mathcal{B}$, this implies $T_{\mathcal{A}}\mathbf{x} = T_{\mathcal{B}}\mathbf{x}, I_{\mathcal{A}}\mathbf{x} = I_{\mathcal{B}}\mathbf{x}, F_{\mathcal{A}}\mathbf{x} = F_{\mathcal{B}}\mathbf{x}$. Hence $|T_{\mathcal{A}}\mathbf{x} - T_{\mathcal{B}}\mathbf{x}| = 0$,$|I_{\mathcal{A}}\mathbf{x} - I_{\mathcal{B}}\mathbf{x}| = 0$, $|F_{\mathcal{A}}\mathbf{x} - F_{\mathcal{B}}\mathbf{x}| = 0$. Thus $Cot_{CSVNS}(\mathcal{A},\mathcal{B}) = 1$.
   Conversely, If $Cot_{CSVNS}(\mathcal{A},\mathcal{B}) = 1$ then $|T_{\mathcal{A}}\mathbf{x} - T_{\mathcal{B}}\mathbf{x}| = 0$,$|I_{\mathcal{A}}\mathbf{x} - I_{\mathcal{B}}\mathbf{x}| = 0$, $|F_{\mathcal{A}}\mathbf{x} - F_{\mathcal{B}}\mathbf{x}| = 0$ since $\tan(0) = 0$.
   So we can we can write, $T_{\mathcal{A}}\mathbf{x} = T_{\mathcal{B}}\mathbf{x}, I_{\mathcal{A}}\mathbf{x} = I_{\mathcal{B}}\mathbf{x}, F_{\mathcal{A}}\mathbf{x} = F_{\mathcal{B}}\mathbf{x}$. Hence $\mathcal{A} = \mathcal{B}$.
3. This proof is obvious.
4. If $\mathcal{A} \subset \mathcal{B} \subset \mathcal{C}$ then $T_{\mathcal{A}}\mathbf{x} \leq T_{\mathcal{B}}\mathbf{x} \leq T_R\mathbf{x}$, $I_{\mathcal{A}}\mathbf{x} \geq I_{\mathcal{B}}\mathbf{x} \geq I_R\mathbf{x}$, and $F_{\mathcal{A}}\mathbf{x} \geq F_{\mathcal{B}}\mathbf{x} \geq F_R\mathbf{x}$ for $\mathbf{x} \in \mathbb{X}$. Now we have the following inequalities:
   $|T_{\mathcal{A}}\mathbf{x} - T_{\mathcal{B}}\mathbf{x}| \leq |T_{\mathcal{A}}\mathbf{x} - T_R\mathbf{x}|$, $|T_{\mathcal{B}}\mathbf{x} - T_R\mathbf{x}| \leq |T_{\mathcal{A}}\mathbf{x} - T_R\mathbf{x}|$;
   $|I_{\mathcal{A}}\mathbf{x} - I_{\mathcal{B}}\mathbf{x}| \leq |I_{\mathcal{A}}\mathbf{x} - T_R\mathbf{x}|$, $|I_{\mathcal{B}}\mathbf{x} - I_R\mathbf{x}| \leq |I_{\mathcal{A}}\mathbf{x} - I_R\mathbf{x}|$;
   $|F_{\mathcal{A}}\mathbf{x} - F_{\mathcal{B}}\mathbf{x}| \leq |F_{\mathcal{A}}\mathbf{x} - F_R\mathbf{x}|$, $|F_{\mathcal{B}}\mathbf{x} - F_R\mathbf{x}| \leq |F_{\mathcal{A}}\mathbf{x} - F_R\mathbf{x}|$;
   Thus $Cot_{CSVNS}(\mathcal{A},\mathcal{C}) \leq Cot_{CSVNS}(\mathcal{A},\mathcal{B})$ and $Cot_{CSVNS}(\mathcal{A},\mathcal{C}) \leq Cot_{CSVNS}(\mathcal{B},\mathcal{C})$. The cotangent function is decreasing function within the interval $[\frac{\pi}{4}, \frac{\pi}{2}]$.

□

5. Encrypted Clustering Framework, Algorithm and Experimental Setup

Encrypted Clustering Framework:
We present a secure clustering framework which combines normalization, homomorphic encryption, PCA and encrypted K-Means clustering. Let $X = \{x_1, ..., x_n\}$, x_i in R^d. Features are scaled to [0,1] and encrypted with a homomorphic encryption. PCA reduces X'W, Encrypted K-Means distributes assignment and update of centroids in clustering in ciphertext space without privacy issues.
Algorithm:
Step 1: Scale data X to [0,1].
Step 2: Use homomorphic encryption to encrypt data.
Step 3: Reduce dataset X using PCA.

Step 4: Use K-Means++ to initialize.
Step 5: Repeat steps of cluster assignment and encrypted centroid update.
Step 6: Use Cotangent CSVNS similarity measure to evaluate.

1. Feature Normalization (Pre-processing Method)

Rule: To ensure that no single feature dominates the distance measurements, all features must be rescaled to a normal distribution (usually 0 to 1). Euclidean distances employed in K-Means on the encrypted space are sectionized in this way.

2. Homomorphic Encryption (Privacy-Preserving Method)

Homomorphic Encryption is a form of encryption protocol used as a privacy-enhancing technique to allow computations to be performed on encrypted data without decryption.

In this research we use the Cheon Kim Kim Song (CKKS) homomorphic encryption scheme, which is constructed to support approximate arithmetic operations on real numbers. We have chosen CKKS because it supports vectorised floating-point operations, efficiently used in machine learning algorithms such as PCA and K-Means clustering methods on encrypted data. The encryption scheme represents all feature values as ciphertexts, enabling operations on encrypted values without the need for decryption. The scheme provides only a few operations, particularly addition and multiplication, and has an approximation error due to the noise and rescaling techniques. The encryption parameters control the trade-offs between computational accuracy and noise in computations.

To ensure consistency and reproducibility of the computations, these cryptographic parameters are adopted:

• Security level: 128-bit classical security
• Polynomial modulus degree (N): 2^{14} (16384)
• Coefficient modulus size: 438 bits (e.g., 60 + 40 + 40 + 40 + 40 + 218 bit chain, depending on rescaling depth)
• Scaling factor (Δ): 2^{40}
• Number of levels: 4-5 multiplicative depth levels (supporting PCA and K-Means operations)

These values balance security, efficiency and precision to allow for secure and stable encrypted computation while maintaining the clustering structure.

Rule: Feature values are encrypted into ciphertexts to allow computations on the encrypted data. The scheme supports only a limited range of operations (such as addition and multiplication) and the encryption parameters must regulate the noise and the loss of precision.

3. Principal Component Analysis (PCA) of dimensionality reduction

Instructions: Project the high-dimensional (encrypted) project data onto the top principal components that have the highest retained variance. Visualization of PC1 and PC2. PC1, PC2, and PC3 should be utilized to maintain more variance if the separation is to be more visualized and more variance is to be captured.

4. Encrypted K-Means Clustering (Normal K-Means)

Rule: This rule is an iterative procedure that is repeated until convergence is achieved: The assignment rule Add up all of the cluster's points that have the closest (encrypted) Euclidean distance to the centroid.

Modify the rule: Every centroid should be recalculated as an average of the points allotted (in cipher form). When the maximum number of iterations is achieved or fewer than one centroid change is obtained, stop.

5. Encrypted K-Means++ Clustering (K-Means with Sage Initialization)

Rule: The initialization is different, but the clustering loop is the same as K-Means:

The first centroid is selected, then squares of the distance to the closest centroid are used to determine the likelihood of selecting other centroids (spreading out centroid). This lessens cold start, increases stability, and speeds up convergence especially when using an encrypted environment.

6. Secure Visualization (Interpretation Method PCA Scatter Plot)

Rule: Only centroid positions, cluster names, and decrypted PCA coordinates (less than three dimensions) are used to plot. The initial high-dimensional characteristics are never revealed.

Experimental Setup:

Data: Iris (150 samples, 4 features).
Normalization: Scaling to [0,1].
Encryption: Homomorphic encryption (additions and multiplications).
Clustering: K-Means, K-Means++, Encrypted K-Means.

Analysis: PCA plot, centroid stability, similarity.

5.1. Cotangent Similarity Measure

Let $T_i = (T_{ik}, I_{ik}, F_{ik})$, $C_j = (T_{jk}, I_{jk}, F_{jk})$ are two CSVNSs. Each set is represented by three components for each feature k:
T_{ik}: Truth-membership of feature $kforT_i$.
I_{ik}: Indeterminacy-membership of feature $kforT_i$.
F_{ik}: Falsity-membership degree of feature $kforT_i$.
The values typically satisfy: $T_{ik}, I_{ik}, F_{ik} \in [0, 1]$
Similarly, for object C_j:
T_{jk}: Truth-membership of feature $kforC_j$.
I_{jk}: Indeterminacy-membership of feature $kforC_j$.
F_{jk}: Falsity-membership degree of feature $kforC_j$.
The values typically satisfy: $T_{jk}, I_{jk}, F_{jk} \in [0, 1]$.
The cotangent similarity measures between T_i and C_j is defined as:
$Cotangent_{CSVNS}(T_i, C_j) =$

$$\frac{1}{n}\sum_{k=1}^{n}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|T_{ik} - T_{jk}| + |I_{ik} - I_{jk}| + |F_{ik} - F_{jk}|)]\}$$

5.2. Multi-Source Signal Based Target Classification via Cotangent Complex Neutrosophic Similarity

This research aims to develop a Cotangent similarity based technique in complex single-valued neutrosophic sets (CSVNS) for the identification of operational targets in multi-source signal data into different operational categories. The data are uncertain, inaccurate and mixed in nature, containing different types of signal information such as radar, thermal and electronics. The proposed method takes into account truth, indeterminacy, and falsity information in the classification process to address this uncertainty.
The method involves using a Cotangent similarity measure to assess the similarity between targets and class templates, and generates similarity scores that allow for ranking and classification of operational targets. The approach offers enhanced ability to deal with noisy, overlapping and uncertain data, and can be used for effective decision-making in surveillance and reconnaissance tasks.
Using the multi-source signal samples $S = \{S_1, S_2, S_3\}$ to accurately categorize the operational targets $T = \{T_1, T_2, T_3\}$ and then applying them to the appropriate operational classes $C = \{C_1, C_2, C_3\}$ is the primary task in the current surveillance and reconnaissance systems. The available information on each target is inherently ambiguous, imprecise, and diverse; it includes heat emissions, radar signatures, electronic monitoring, and other signal measures. This uncertainty necessitates a mathematical procedure that can simultaneously handle truth, indeterminacy, and falsity. The relationship between targets, signals, and classes in a multifaceted environment is related in terms of event-based measures (e) and their corresponding measures in the operational classification table (Table 2). However, overlapping values, inconsistent reliability, and nonlinear relationships between features make it impossible to directly compare a response of raw signals between targets and classes. This is resolved by proposing a Cotangent similarity measure based on the complex neutrosophic soft set (Cotangent CSVNS) framework, which enables the measurement of each target-class pair's similarity. It considers the joint contribution of the truth-membership, indeterminacy-membership, and falsity-membership functions, normalized with respect to $n = 3$ attributes, in each pair (T_i, C_j). Cotangent similarity scores are generated as a result, and these can be used to rank candidate target profiles in relation to operational class templates.

Table 1. Matrix of Target Intelligence Features Based on Cotangent Similarity ($T \times S$)

	S_1	S_2	...	S_n
T_1	T_{11}, I_{11}, F_{11}	T_{12}, I_{12}, F_{12}	...	T_{1n}, I_{1n}, F_{1n}
T_2	T_{21}, I_{21}, F_{21}	T_{22}, I_{22}, F_{22}	...	T_{2n}, I_{2n}, F_{2n}
...	...	...	...	...
T_m	T_{m1}, I_{m1}, F_{m1}	T_{m2}, I_{m2}, F_{m2}	...	T_{mn}, I_{mn}, F_{mn}

Table 2. Operational Classification Matrix for Target Surveillance Data ($T \times S \to C$)

Row-I	S_1	S_2	S_3	**Row-II**	C_1	C_2	C_3
T_1	$\begin{pmatrix}0.5e^{\iota\pi(0.6)}\\0.7e^{\iota\pi(0.5)}\\0.3e^{\iota\pi(0.3)}\end{pmatrix}$	$\begin{pmatrix}0.6e^{\iota\pi(0.7)}\\0.4e^{\iota\pi(0.4)}\\0.3e^{\iota\pi(0.4)}\end{pmatrix}$	$\begin{pmatrix}0.3e^{\iota\pi(0.2)}\\0.5e^{\iota\pi(0.5)}\\0.8e^{\iota\pi(0.3)}\end{pmatrix}$	S_1	$\begin{pmatrix}0.3e^{\iota\pi(0.4)}\\0.5e^{\iota\pi(0.7)}\\0.7e^{\iota\pi(0.7)}\end{pmatrix}$	$\begin{pmatrix}0.7e^{\iota\pi(0.6)}\\0.6e^{\iota\pi(0.5)}\\0.2e^{\iota\pi(0.3)}\end{pmatrix}$	$\begin{pmatrix}0.5e^{\iota\pi(0.8)}\\0.4e^{\iota\pi(0.7)}\\0.9e^{\iota\pi(0.3)}\end{pmatrix}$
T_2	$\begin{pmatrix}0.4e^{\iota\pi(0.6)}\\0.7e^{\iota\pi(0.9)}\\0.5e^{\iota\pi(0.7)}\end{pmatrix}$	$\begin{pmatrix}0.2e^{\iota\pi(0.4)}\\0.4e^{\iota\pi(0.9)}\\0.6e^{\iota\pi(0.3)}\end{pmatrix}$	$\begin{pmatrix}0.7e^{\iota\pi(0.7)}\\0.4e^{\iota\pi(0.3)}\\0.6e^{\iota\pi(0.6)}\end{pmatrix}$	S_2	$\begin{pmatrix}0.2e^{\iota\pi(0.5)}\\0.3e^{\iota\pi(0.2)}\\0.7e^{\iota\pi(0.3)}\end{pmatrix}$	$\begin{pmatrix}0.6e^{\iota\pi(0.6)}\\0.7e^{\iota\pi(0.8)}\\0.4e^{\iota\pi(0.3)}\end{pmatrix}$	$\begin{pmatrix}0.3e^{\iota\pi(0.6)}\\0.6e^{\iota\pi(0.7)}\\0.8e^{\iota\pi(0.9)}\end{pmatrix}$
T_3	$\begin{pmatrix}0.7e^{\iota\pi(0.9)}\\0.6e^{\iota\pi(0.5)}\\0.8e^{\iota\pi(0.8)}\end{pmatrix}$	$\begin{pmatrix}0.2e^{\iota\pi(0.4)}\\0.8e^{\iota\pi(0.5)}\\0.7e^{\iota\pi(0.6)}\end{pmatrix}$	$\begin{pmatrix}0.6e^{\iota\pi(0.9)}\\0.3e^{\iota\pi(0.6)}\\0.2e^{\iota\pi(0.3)}\end{pmatrix}$	S_3	$\begin{pmatrix}0.4e^{\iota\pi(0.4)}\\0.7e^{\iota\pi(0.5)}\\0.5e^{\iota\pi(0.9)}\end{pmatrix}$	$\begin{pmatrix}0.6e^{\iota\pi(0.2)}\\0.3e^{\iota\pi(0.5)}\\0.4e^{\iota\pi(0.4)}\end{pmatrix}$	$\begin{pmatrix}0.7e^{\iota\pi(0.2)}\\0.3e^{\iota\pi(0.8)}\\0.2e^{\iota\pi(0.3)}\end{pmatrix}$

The cotangent similarity measures between T_i and C_j is defined as:
$Cotangent_{CSVNS}(T_i, C_j) =$

$$\frac{1}{n}\sum_{k=1}^{n}\{\cot[\frac{\pi}{4}+\frac{\pi}{12}(|T_{ik}-T_{jk}|+|I_{ik}-I_{jk}|+|F_{ik}-F_{jk}|)]\}$$

For $n = 3$ then $R_1 + C_1 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\frac{1}{n}\sum_{i=1}^{n}\{\cot[\frac{\pi}{4}+\frac{\pi}{12}(|T_{Mi}-T_{Ni}|+|I_{Mi}-I_{Ni}|+|F_{Mi}-F_{Ni}|)]\}$$

$$\begin{aligned}
&= \frac{1}{3}\{\cot[\frac{\pi}{4}+\frac{\pi}{12}(|(-0.1545+0.4755\iota)-(0.0927+0.2857\iota)|+\\
&|(0+0.7\iota)-(-0.1545+0.4755\iota)|+|(0.1765+0.2427\iota)-(-0.2164+0.6657\iota)|)]\}\\
&+\frac{1}{3}\{\cot[\frac{\pi}{4}+\frac{\pi}{12}(|(-0.3527+0.4854\iota)-(0+0.2\iota)|+\\
&|(0.1236+0.3804\iota)-(0.2427+0.1763\iota)|+|(0.0927+0.2875\iota)-(0.4114+0.5663\iota)|)]\}\\
&+\frac{1}{3}\{\cot[\frac{\pi}{4}+\frac{\pi}{12}(|(0.2427+0.1763\iota)-(0.1236+0.3804\iota)|+\\
&|(0+0.5\iota)-(0+0.7\iota)|+|(0.4702+0.6472\iota)-(-0.4755+0.1545\iota)|)]\}\\
&= 0.1740+0.1794+0.1377 = 0.4913
\end{aligned}$$

For $n = 3$ then $R_1 + C_2 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\begin{aligned}
&\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.1545 + 0.4755\iota) - (-0.2163 + 0.6657\iota)|+ \\
&|(0 + 0.7\iota) - (0 + 0.6\iota)| + |(0.1765 + 0.2427\iota) - (0.1175 + 0.1618\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.3527 + 0.4854\iota) - (0.1854 + 0.5706\iota)|+ \\
&|(0.1236 + 0.3804\iota) - (0.2163 + 0.6657\iota)| + |(0.0927 + 0.2875\iota) - (0.2311 + 0.3236\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.2427 + 0.1763\iota) - (0.4854 + 0.3526\iota)|+ \\
&|(0 + 0.5\iota) - (0 + 0.3\iota)| + |(0.4702 + 0.6472\iota) - (0.1236 + 0.3804\iota)|)]\} \\
&= 0.2699 + 0.1938 + 0.1998 = 0.6635
\end{aligned}$$

For $n = 3$ then $R_1 + C_3 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\begin{aligned}
&\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.1545 + 0.4755\iota) - (-0.4045 + 0.2939\iota)|+ \\
&|(0 + 0.7\iota) - (-0.2351 + 0.3236\iota)| + |(0.1765 + 0.2427\iota) - (0.5290 + 0.7281\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.3527 + 0.4854\iota) - (0.0927 + 0.2853\iota)|+ \\
&|(0.1236 + 0.3804\iota) - (0.3527 + 0.4859\iota)| + |(0.0927 + 0.2875\iota) - (-0.7609 + 0.2472\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.2427 + 0.1763\iota) - (0.5663 + 0.4115\iota)|+ \\
&|(0 + 0.5\iota) - (-0.2427 + 0.1763\iota)| + |(0.4702 + 0.6472\iota) - (0.1176 + 0.1618\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.2781 + 0.8560\iota) - (-0.3804 + 0.1236\iota)|+ \\
&|(0.0618 + 0.1902\iota) - (0 + 0.3\iota)| + |(0.2351 + 0.3236\iota) - (0.7609 + 0.2472\iota)|)]\} \\
&= 0.1533 + 0.1284 + 0.1479 = 0.5785
\end{aligned}$$

For $n = 3$ then $R_2 + C_1 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\begin{aligned}
&\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.1236 + 0.3804\iota) - (0.0927 + 0.2857\iota)|+ \\
&|(-0.6658 + 0.2163\iota) - (-0.1545 + 0.4755\iota)| + |(0.2939 + 0.4045\iota) - (-0.2164 + 0.6657\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.0618 + 0.1902\iota) - (0 + 0.2\iota)|+ \\
&|(-0.3804 + 0.1236\iota) - (0.2427 + 0.1763\iota)| + |(0.3527 + 0.4854\iota) - (0.4114 + 0.5663\iota)|)]\} \\
&+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.0927 + 0.2853\iota) - (0.1236 + 0.3804\iota)|+ \\
&|(0.1236 + 0.3804\iota) - (0 + 0.7\iota)| + |(0.1545 + 0.4755\iota) - (-0.4755 + 0.1545\iota)|)]\} \\
&= 0.1502 + 0.1604 + 0.2179 = 0.5287
\end{aligned}$$

For $n = 3$ then $R_2 + C_2 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.1236 + 0.3804\iota) - (-0.2163 + 0.6657\iota)|+ |(-0.6658 + 0.2163\iota) - (0 + 0.6\iota)| + |(-0.2939 + 0.4045\iota) - (0.1175 + 0.1618\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.0618 + 0.1902\iota) - (0.1854 + 0.5706\iota)|+ |(-0.3804 + 0.1236\iota) - (0.2163 + 0.6657\iota)| + |(0.3527 + 0.4854\iota) - (0.2311 + 0.3236\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.0927 + 0.2853\iota) - (0.4854 + 0.3526\iota)|+ |(0.1236 + 0.3804\iota) - (0 + 0.3\iota)| + |(0.1545 + 0.4755\iota) - (0.1236 + 0.3804\iota)|)]\}$$
$$= 0.1333 + 0.2128 + 0.1475 = 0.4937$$

For $n = 3$ then $R_2 + C_3 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.1236 + 0.3804\iota) - (-0.4045 + 0.2939\iota)|+ |(-0.6658 + 0.2163\iota) - (-0.2351 + 0.3236\iota)| + |(-0.2939 + 0.4045\iota) - (0.5290 + 0.7281\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.0618 + 0.1902\iota) - (0.0927 + 0.2853\iota)|+ |(-0.3804 + 0.1236\iota) - (0.3527 + 0.4859\iota)| + |(0.3527 + 0.4854\iota) - (-0.7609 + 0.2472\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.0927 + 0.2853\iota) - (0.5663 + 0.4115\iota)|+ |(0.1236 + 0.3804\iota) - (-0.2427 + 0.1763\iota)| + |(0.1545 + 0.4755\iota) - (0.1176 + 0.1618\iota)|)]\}$$
$$= 0.1257 + 0.1477 + 0.0830 = 0.3576$$

For $n = 3$ then $R_3 + C_1 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.6658 + 0.2163\iota) - (0.0927 + 0.2857\iota)|+ |(0 + 0.6\iota) - (-0.1545 + 0.4755\iota)| + |(-0.6472 + 0.4702\iota) - (-0.2164 + 0.6657\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.0618 + 0.1902\iota) - (0 + 0.2\iota)|+ |(0 + 0.8\iota) - (0.2427 + 0.1763\iota)| + |(-0.2163 + 0.6658\iota) - (0.4114 + 0.5663\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.5707 + 0.1854\iota) - (0.1236 + 0.3804\iota)|+ |(-0.0927 + 0.2853\iota) - (0 + 0.7\iota)| + |(0.1176 + 0.1618\iota) - (-0.4755 + 0.1545\iota)|)]\}$$
$$= 0.1449 + 0.1141 + 0.1528 = 0.4110$$

For $n = 3$ then $R_3 + C_2 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.6658 + 0.2163\iota) - (-0.2163 + 0.6657\iota)|+ |(0 + 0.6\iota) - (0 + 0.6\iota)| + |(-0.6472 + 0.4702\iota) - (0.1175 + 0.1618\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.0618 + 0.1902\iota) - (0.1854 + 0.5706\iota)|+ |(0 + 0.8\iota) - (0.2163 + 0.6657\iota)| + |(-0.2163 + 0.6658\iota) - (0.2311 + 0.3236\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.5707 + 0.1854\iota) - (0.4854 + 0.3526\iota)|+ |(-0.0927 + 0.2853\iota) - (0 + 0.3\iota)| + |(0.1176 + 0.1618\iota) - (0.1236 + 0.3804\iota)|)]\}$$
$$= 0.1421 + 0.1503 + 0.1678 = 0.4604$$

For $n = 3$ then $R_3 + C_3 \Rightarrow \cot_{CSVNS}(T_i, C_j) =$

$$\frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.6658 + 0.2163\iota) - (-0.4045 + 0.2939\iota)|+$$
$$|(0 + 0.6\iota) - (-0.2351 + 0.3236\iota)| + |(-0.6472 + 0.4702\iota) - (0.5290 + 0.7281\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(0.0618 + 0.1902\iota) - (0.0927 + 0.2853\iota)|+$$
$$|(0 + 0.8\iota) - (0.3527 + 0.4859\iota)| + |(-0.2163 + 0.6658\iota) - (-0.7609 + 0.2472\iota)|)]\}$$
$$+ \frac{1}{3}\{\cot[\frac{\pi}{4} + \frac{\pi}{12}(|(-0.5707 + 0.1854\iota) - (0.5663 + 0.4115\iota)|+$$
$$|(-0.0927 + 0.2853\iota) - (-0.2427 + 0.1763\iota)| + |(0.1176 + 0.1618\iota) - (0.1176 + 0.1618\iota)|)]\}$$
$$= 0.1045 + 0.1633 + 0.1542 = 0.4221$$

All target-classification pairings are then averaged by adding the cotangent values that were determined for each pair of targets and categorized profiles.
The values of the resulting cotangent similarity:
$Cotangent_{CSVNS}(T_1, C_1) = 0.4913$
$Cotangent_{CSVNS}(T_1, C_2) = 0.6653$
$Cotangent_{CSVNS}(T_1, C_3) = 0.5785$
$Cotangent_{CSVNS}(T_2, C_1) = 0.5287$
$Cotangent_{CSVNS}(T_2, C_2) = 0.4937$
$Cotangent_{CSVNS}(T_2, C_3) = 0.3576$
$Cotangent_{CSVNS}(T_3, C_1) = 0.4110$
$Cotangent_{CSVNS}(T_3, C_2) = 0.4604$
$Cotangent_{CSVNS}(T_3, C_3) = 0.4221$

Table 3. Cotangent Similarity scores between signal samples $(S_1 - S_3)$ and class templates $(T_1 - T_3)$

Cot SM	S_1	S_2	S_3
T_1	0.4913	0.6653	0.5785
T_2	0.5287	0.4937	0.3576
T_3	0.4110	0.4604	0.4221

Table 4. Iris-Style Dataset (From Cotangent Similarity Matrix)

Sepal Length	**Sepal Width**	**Petal Length**	**Petal Width**	**Species**
0.4913	0.6653	0.5785	-	Setosa
0.5287	0.4937	0.3576	-	Versicolor
0.4110	0.4604	0.4221	-	Virginica

Important Note:
- We have 3 features in our original data (S_1, S_2, S_3).
- We mapped them to:
  - Sepal Length $\rightarrow S_1$
  - Sepal Width $\rightarrow S_2$
  - Petal Length $\rightarrow S_3$
- There is no value for Petal Width, so we leave it blank (-).

6. Result and Discussion

The scatter plot of Figure 1 illustrates the Encrypted K-Means Clustering with a 2D PCA (Principal Component Analysis) projection. Each point in the table represents a coded instance of data cast into two major dimensions: PCA Component 1 (x-axis) and PCA Component 2 (y-axis). These axes represent the significant directions of variation in the encrypted feature space, enabling the visualization of the separation of clusters in low dimensions. The clusters are color-coded to follow three encrypted clusters that the K-Means algorithm could identify:
Blue: Cluster 1
Orange: Cluster 2
Green: Cluster 3

Figure 1. Encrypted K-Means Clustering with 2D PCA Projection

In general, the PCA-reduced plane shows the distribution of clusters in relation to the plot. The dispersion of Cluster 1 (blue) is primarily found in the lower-right quadrant, Cluster 2 (orange) in the upper-central region, and Cluster 3 (green) on the left side of the plane. The black system's centroid markers represent encrypted meanings of each cluster's placements, and the observation of different centers with minimal overlaps verifies the successful separation of the encrypted clustering process. The K-Means clustering method was able to identify natural structural trends and grouping behavior in the data despite the fact that the entire data set was encrypted. Without altering the clusters' intrinsic topology, the PCA transformation provides a useful low-dimensional representation of the encrypted feature associations. This example demonstrates that encryption has no effect on analytical capacity; the encrypted feature space retains its behavioral clusters while maintaining anonymity. The apparent distances between the centers show a substantial inter-group discontinuity, while the clusters show internal consistent links.
As a result, the Encrypted K-Means Clustering (2D PCA Visualization) is a useful technique to demonstrate that unsupervised learning is possible on encrypted data, and that it is possible to find patterns, maintain the structure, and perform analytics (analyses) without disclosing any raw or sensitive values.

The encrypted and normalized K-Means clustering, which is projected using a 2D PCA (Principal Component Analysis) representation, is displayed in the scatter plot in Figure 2. Between the two primary components of PCA Component 1 (x-axis) and PCA Component 2 (y-axis), the points correspond to a normalized encrypted sample of data. The most important directions of variance in the encrypted normalized feature space are represented by these components, which enable the visualization of cluster boundaries and separations. The K-Means technique detects three distinct encrypted clusters, which are indicated by color-coding the data values:
Cluster 1 is shown by red
Cluster 2 by yellow
Cluster 3 by green
the centers of gravity are indicated by black **x**.

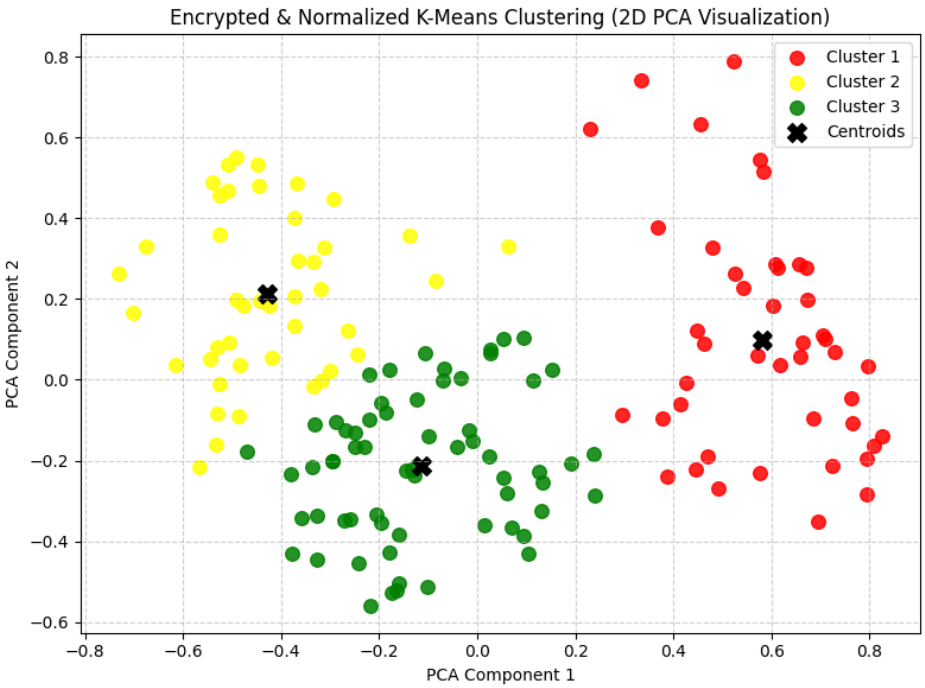

Figure 2. Encrypted & Normalized K-Means Clustering with 2D PCA Projection

High spatial distances between the clusters are shown in the data visualization, indicating good classification in the encrypted-normalized space. Cluster 1 (red) is a close-knit group that is situated on the right. Cluster 3 (green) is situated in the lower-central region with mild dispersion, whereas Cluster 2 (yellow) is situated in the upper-left region with moderately spread points. A striking indication of a well-defined clustering structure is the black centroid, which are distinct between cluster areas and represent the encrypted means position of each group. Normalization ensures that all data dimensions are normalized to a common 0-1 interval before encryption, balancing the K-Means method's distance computations. Although the true magnitudes are concealed behind an encryption layer and may not be visible, coherent structural and relational concerns can be divided. The capacity of the secure model of analysis to preserve interpretability and cluster integrity is demonstrated by this Encrypted and Normalized K-Means Clustering (2D PCA Visualization). Confidential clustering, structural analysis, and secure visual interpretations without disclosing any underlying feature values are made possible by this confirmation that encrypted normalized data may be exposed to un-monitored learning algorithms without losing its privacy.

The Encrypted 3D K-Means Clustering of the Iris dataset is shown in Figure 3, a 3D scatter plot that has been projected on three primary components using Principal Component Analysis (PCA). The primary variance trends in the encrypted dataset are represented by the PCA Components 1, 2, and 3 when the encrypted data points are

shown in the reduced feature space. The data points' clusters are color-coded and encrypted:
Cluster 1 is shown by red
Cluster 2 by yellow
Cluster 3 by green
the encrypted cluster center is indicated by black **x** markers.

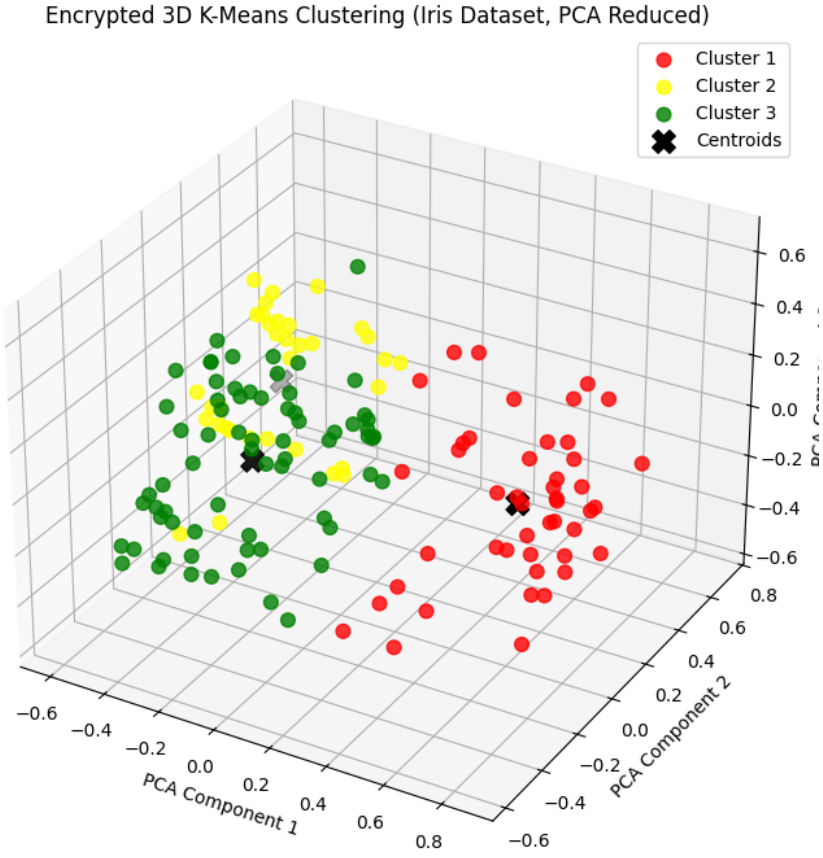

Figure 3. Encrypted 3D K-Means Clustering of the Iris dataset

There is a distinct three-dimensional separation between the clusters in the picture. The lower-right portion of the plot is home to Cluster 1 (red), the upper-central plane is home to Cluster 2 (yellow), and the left-lower quadrant is home to Cluster 3 (green). The centroid's good separation indicates the formation of distinct, well-separated groupings. Even in a low-dimension and encrypted feature space, the encrypted clustering algorithm effectively preserves the borders between clusters, as seen by the geometric distance between the centroid. Even if the entire dataset is encrypted, the PCA-reduced projection retains the relational geometry of the original data distribution. It was discovered that applying the encrypted domain to the K-Means method preserved the security of the data while identifying similar structures present in the un encrypted dataset. This Encrypted 3D K-Means Clustering (PCA Reduced) visualization highlights the potential for using unsupervised learning while maintaining anonymity. It demonstrates how dimensionality reduction and clustering, in spite of encryption, maintain pattern integrity, class separation, and centroid separation, enabling the investigation of high-dimensional relationships while concealing any sensitive numerical data.

The Encrypted & Normalized 3D K-Means Clustering of the Iris dataset after dimensionality reduction using Principal Component Analysis (PCA) is shown in Figure 4, a 3D scatter plot. Plotted on three primary axes (PCA

1, PCA 2, and PCA 3), each point represents a normalized and encrypted sample of the data set that reflects the dominant variance pattern in the encrypted feature space. K-Means encrypted clusters are used to arrange and color-code the data points:
Cluster 1 is represented by yellow
Cluster 2 by blue
Cluster 3 by pink
Black **x** markers: Each cluster's center ciphers.

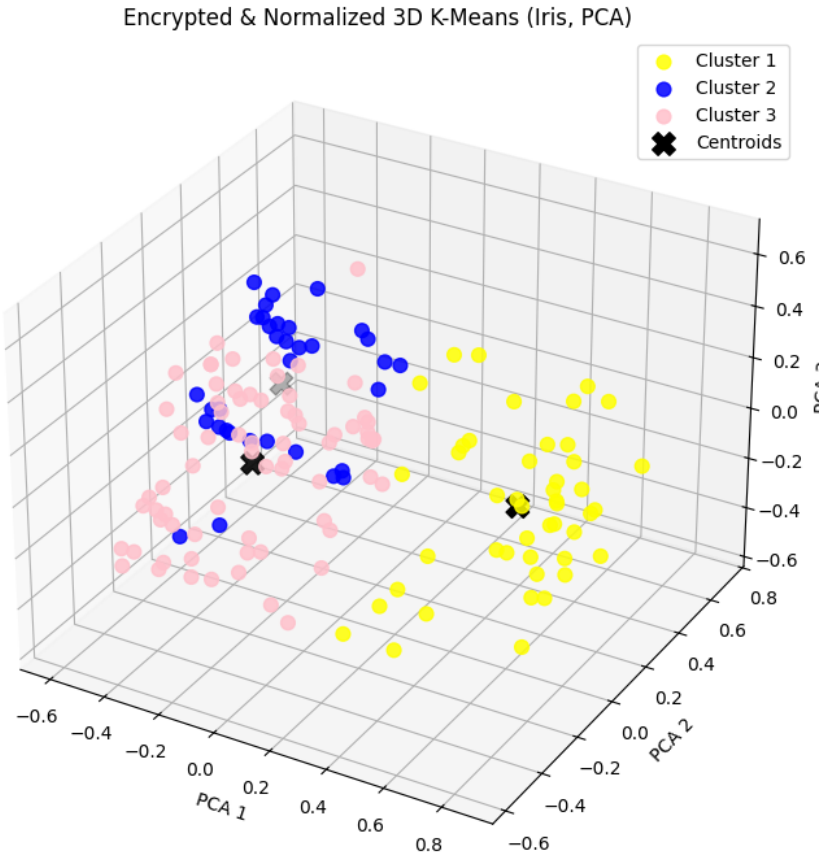

Figure 4. Encrypted & Normalized 3D K-Means Clustering of the Iris dataset

Excellent spatial segmentation of the three encrypted groups is displayed in the graph. Cluster 1 (yellow) has a tight cluster in the lower-right corner, Cluster 2 (blue) has a dense cluster in the upper-left volume, and Cluster 3 (pink) partially connects the two extremes by flowing across the center region. Additionally, the centroid are positioned clearly, indicating limited inter-cluster overlap and good encrypted partitioning. Prior to encryption, normalization ensures that all feature magnitudes are consistent within a range of 0-1, improving clustering accuracy and stabilizing distance-related computations in the encrypted space. While PCA enables data visualization by projecting the encrypted high-dimensional space into three comprehensible axes, the K-Means technique operates on encrypted-normalized vectors while maintaining the structural coherence of natural groupings. The Encrypted and Normalized 3D K-Means (Iris, PCA) plot generally demonstrates that meaningful grouping can be achieved even with rigorous encryption and normalization. Additionally, it verifies that the encrypted data does not interfere with its original form and permits privacy-sensitive cluster finding, inter-group differentiation, and centroid separation without disclosing any sensitive or original numerical data.

Figure 5's Encrypted K-Means++ Clustering of the Iris dataset is a two-dimensional PCA scatter plot of the data. Each point's encrypted data sample is projected onto the first two Principal Components (PCA Component 1 and PCA Component 2), which account for most of the linear variance in the encrypted feature distribution. Each color represents an encrypted cluster assignment, and the depiction is based on the K-Means++ algorithm with improved centroid initialization with encryption:
Cluster 1 is represented by blue
Cluster 2 by orange
Cluster 3 by green
the clusters cryptic cores are indicated by black **x** markings.

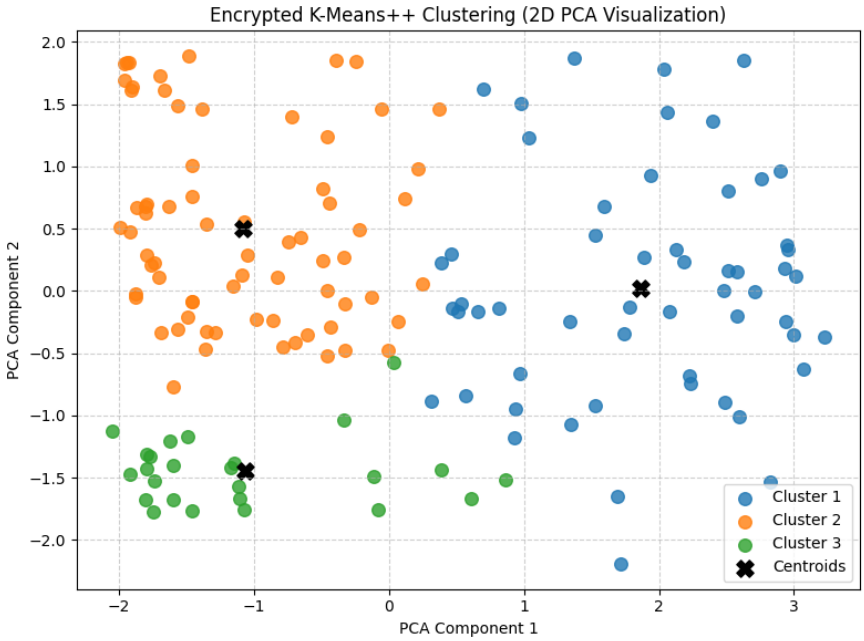

Figure 5. Encrypted K-Means++ Clustering of the Iris dataset

The PCA projection makes it simple to classify the clustering structure. Cluster 1 (blue) is positioned on the right side of the plane, indicating a significant concentration of instances at higher PCA-1 values. Cluster 2 (orange), which is wide and related along intermediate PCA ranges, dominates the upper-left region. Cluster 3 (green), a distinct group with decreased variance in PCA-2, is situated in the lower-left quadrant. Strong initialization and low partition intersection are demonstrated by the centroids' highly effective placement at the geometric centers of the corresponding clusters. By (i) ensuring that the centroid is initialized with spatially varying encrypted sites, which reduces iteration instability and the local minimum, the K-Means++ initialization enhances the convergence qualities. The 2D PCA projection maintains the relative spatial relationships showing the distinct cluster boundaries while safeguarding the original numerical values, even while the entire dataset is fully encrypted. Overall, this Encrypted K-Means++ (2D PCA Visualization) shows that large geometric distances between clusters may still be retained even with encrypted dimensionally reduced data. The results verify that privacy-preserving clustering during optimal centroid initialization is successful in preserving intra-cluster integrity and inter-cluster separation; pattern-finding may be done without disclosing any data.

After reducing the dimensionality using the Principal Component Analysis (PCA) tool, Figure 6 displays the encrypted and normalized 3D K-Means++ Clustering of the Iris data. The first three major or principal components of PCA 1, PCA 2, and PCA 3, which together provide the highest variance structure of the encrypted data distribution, form the three-dimensional subspace in which the data points encrypted and normalized instances of data are shown. In order to increase centroid placement stability, data points are color-coded and their encrypted

cluster assignments are calculated using the K-Means++ initialization algorithm:
Black, with white borders
x: Encrypted centroid
Yellow: Cluster 1
Black: Cluster 2
Sky Blue: Cluster 3.

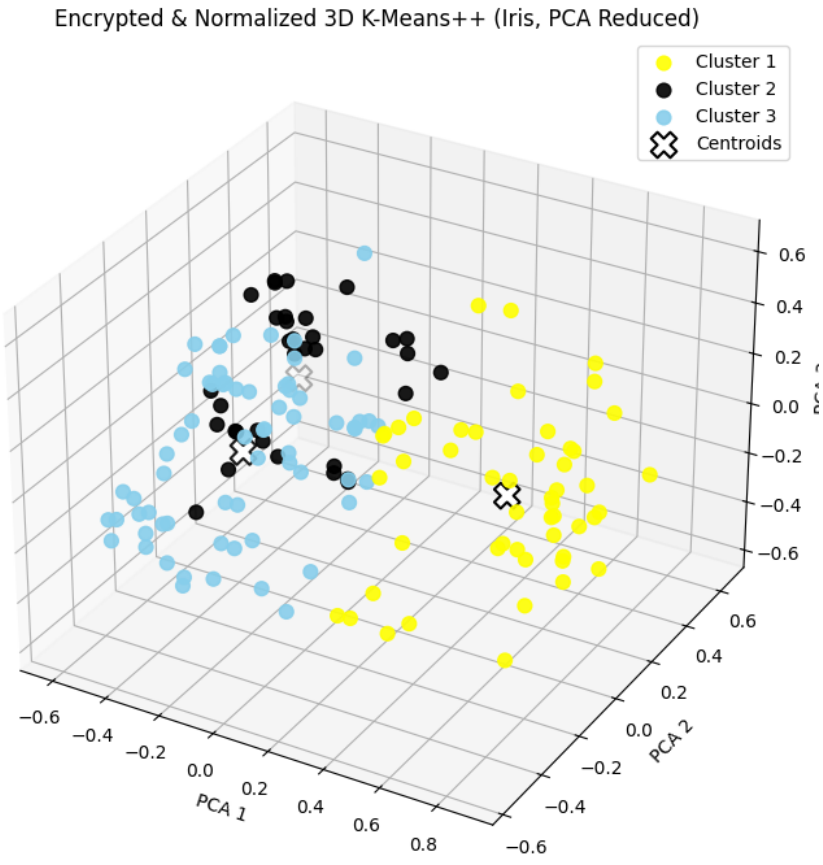

Figure 6. Encrypted & Normalized 3D K-Means++ Clustering of the Iris data

There are discrete, non-overlapping cluster sections in the visualization. The plot's right-hand side is dominated by cluster 1 (yellow), which is dispersed cohesively and densely. While Cluster 3 (sky blue) establishes an intermediate zone between the two other clusters, Cluster 2 (black) occupies the upper-left spatial domain with a small, vertically dispersed pattern. There is sufficient initializing and inter-cluster separation between the encrypted and normalized data, and the centroid are clearly separated. In the case of encrypted domains, where value magnitude cannot be used to directly initialize the centroid, the model with the addition of K-Means++ enables the centroid to be initialized with the optimal spatial diversity to prevent the convergence to suboptimal partitions. Encrypted distances are both computationally and semantically stable, and normalization also standardizes feature scales. The combined efficacy of three secure levels of analytical activity encryption, normalization, and optimal centroid initiation is demonstrated in this Encrypted and Normalized 3D K-Means++ (Iris, PCA Reduced) figure. Together, they provide a geometrically coherent clustering structure that PCA can interpret in the space of decreased dimensionality. The results demonstrate the availability of encrypted-normalized learning pipelines that

can replicate significant grouping and boundary accuracy, allowing for safe, privacy-sensitive clustering without compromising spatial accuracy or analysis quality.

The Encrypted 3D K-Means Clustering on the Iris data, which had undergone a dimensionality reduction using Principal Component Analysis (PCA), is displayed in the 3D scatter diagram in Figure 7. The three dimensions that correspond to PCA Component 1, PCA Component 2, and PCA Component 3 are combined to express the essence of variance and structure of the encrypted data set. Each point is an encrypted and PCA-projected point of the three-dimensional space. Based on the K-Means clustering, the data clusters are categorized into several groups and color-coded as follows:

Black X markers: Encrypted centroids of each cluster's geometric centers

Red: Cluster 1

Yellow: Cluster 2

Green: Cluster 3.

The map displays well-differentiated, dispersed clusters in the three-dimensional PCA reduced space. Cluster 1

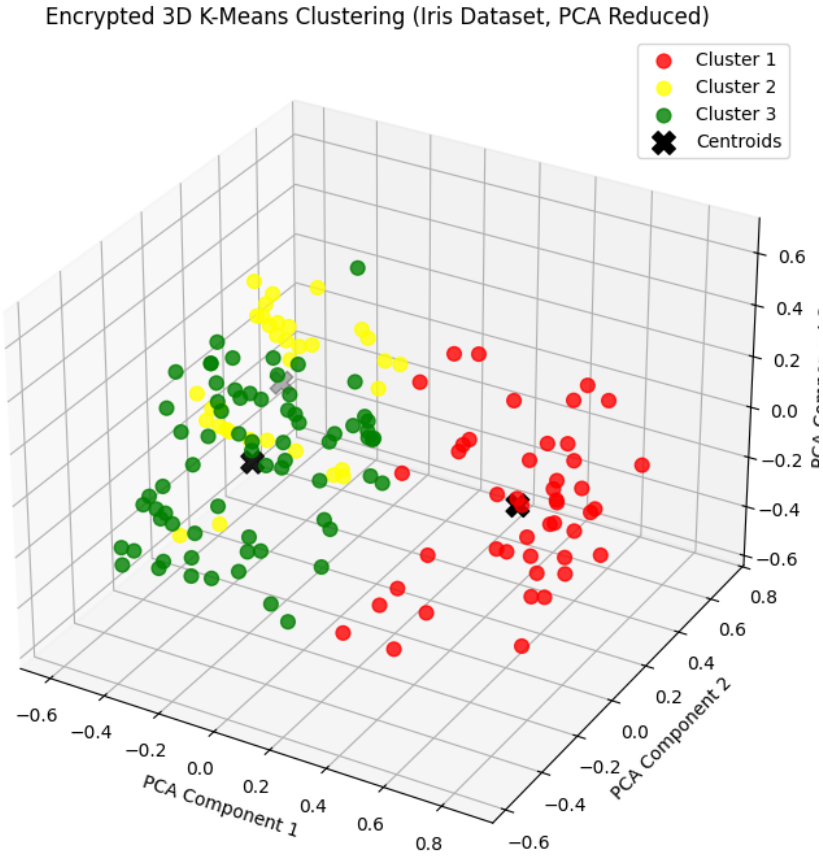

Figure 7. Encrypted 3D K-Means Clustering on the Iris data

(red) appears to be near the centroid on the right. In contrast to Cluster 3 (green), which is located on the left-lower portion and has a wider distribution but is clearly defined by the other two clusters, Cluster 2 (yellow) is centered on the upper section and is reasonably dense. Even when the clusters are encrypted, there is a significant inter-cluster separation and a balanced division since the centroid are symmetrically positioned and visibly separated. PCA reduction simplifies the high dimensional encrypted data while preserving the most informative variance qualities that allow for accurate clustering and effective visualization in a compressed format. The encryption layer suggests

that while all original values are hidden, the geometrical structure between clusters is preserved; in other words, the distance values and clustering structure are preserved in encrypted space. The capacity of encrypted analytic models to preserve spatial separability, centroid accuracy, and cluster integrity in a multidimensional privacy-preserving setting is confirmed by this Encrypted 3D K-Means Clustering (Iris, PCA Reduced) visualization. The results show that K-Means may successfully display intrinsic data clusters despite encryption and PCA compression, allowing for the achievement of secure, interpretable, and geometry-compatible clustering results without disclosing sensitive underlying information.

The Normalized Encrypted K-Means++ Clustering of the Iris dataset is displayed on a 2D PCA projection on the scatter plot in Figure 8. Each encrypted and normalized piece of data is represented by the points, which are plotted in the two main PCA components, PCA Component 1 and PCA Component 2, which show the most important structure of the variance in the encrypted and normalized feature space. These clusters' encrypted K-Means++ assignments are used to determine their color:
Cluster 1 is represented by red
Cluster 2 by yellow
Cluster 3 by green
Black **x**, markers: comprised the clusters' centroid encryptions.

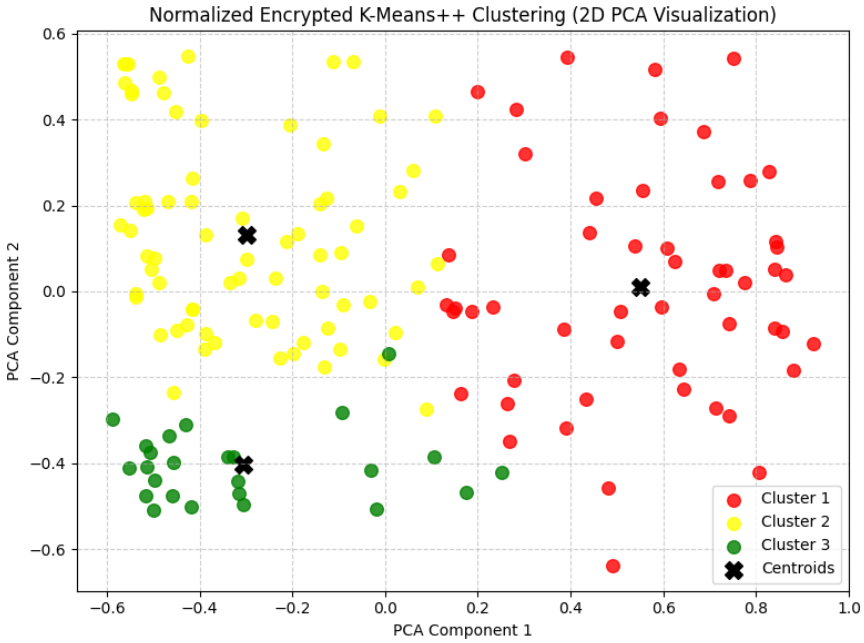

Figure 8. Normalized & Encrypted K-Means Clustering of the Iris data

The clustering structure shows that the group borders are distinct and well-separated. Cluster 1 (red) is a dense, uniform cluster that extends on the right side of the PCA plane. While Cluster 3 (green) is the largest cluster occupying the bottom-left half, suggesting that the features are distinct after normalization, Cluster 2 (yellow) is the largest cluster occupying the left-upper part in a compact way. Even in the encrypted state, the centroid are at the center of their respective clusters, and both intra-cluster consistency and centroidal alignment are strong. In order to preserve the consistency of the distance calculations and lessen the distortion brought on by the different values, the normalization step normalizes all the feature values to a consistent range [0 1] before encryption. Meanwhile, by selecting a range of beginning points to boost convergence efficiency and cluster stability, the K-Means++ initialization can be utilized to enhance centroid location. This Normalized Encrypted K-Means++ (2D PCA Visualization) effectively demonstrates that important geometric correlations and separability may be preserved

using data normalization, encryption, and clustering initialization optimization. It has been demonstrated that the privacy-preserving analytical models are able to maintain interpretive clarity, cluster compactness, and centroidal balance even under full encryption, without disclosing any underlying numerical information. Despite this, the normalized form of projection still exhibits notable structural differences between the clusters.

7. Method-based Analysis, Aspect-based Analysis, and Sensitivity Analysis

7.1. Method-based Analysis

Based on the methodological approach, a multi-stage machine learning pipeline that protects privacy supports the visualizations. The following is a methodical breakdown of the primary methodology:

Stage 1: Data Pre-processing: Two potential surgeries are mentioned in this first step. In order to prevent any feature from dominating the final distance calculation, normalization (used in Figures 2, 4, 5, and 7) converts all original feature values into normalized values (e.g., [0,1]). This is crucial for encrypted computation since results could be skewed by size differences. This is then encrypted, in which each data feature is turned into ciphertexts based on either a Fully Homomorphic Encryption (FHE) or a Partial Homomorphic Encryption scheme [12]. This converts the dataset to an encrypted feature space in which all the analytical operations are going to be done.

Stage 2: Reduction of dimension through the use of PCA: The encrypted data is subjected to Principal Component Analysis. This is distinguished by the computation of the covariance matrix and its eigenvectors/eigenvalues in the encrypted domain using linear algebraic security protocols. The result is an approximation of the high-dimensional encrypted data to a 2D or 3D lower-dimensional subspace, represented by the principal components that add the most variance. This step has two benefits:

(a). it requires less computing power because of clustering and visualization;

(b). it provides an interpretable geometric interpretation of the encrypted data's structure.

Stage 3: K-Means Clustering encryption: The fundamental clustering technique only functions on encrypted data. Its cycle is iterative:

(a). Task The closest encrypted centroid-based encrypted Euclidean distance calculation is assigned to each encrypted data point.

(b). Revise The encrypted mean of all the points assigned to that cluster is used to recalculate the centroids. Either the conventional K-Means (Figures 1, 3, 4, 8) or the K-Means++ (Figures 5, 6, 7) are used in this step. K-Means++ modifies the second step and starts a probabilistic approach to select distant points as the algorithm's initial centers in order to improve the convergence quality [16, 17].

Stage 4: Visualizing and Interpreting: The centroid coordinates and overall encrypted cluster assignments are only decrypted for visualization. Color-coded cluster labels are used in a 2D/3D graphic of the PCA positions of each point and centroid. The projected coordinates and cluster IDs are the only plaintext data that may be displayed in this presentation; the high-dimensional feature values are always unknown.

The process of methodology: Unprocessed Data (Normalization) Cryptography PCA that is encrypted Clustering using Encryption A sequential flow of privacy-preserving unsupervised learning is indicated by encrypted visualization.

7.2. Aspect-based Analysis

The results of a concept-based analysis are categorized based on the main conceptual factors that impact the privacy-saving strategies.

Aspect 1: Geometric Separation & Geometric Integrity

Observation: The space of PCA projections is clearly divided in all eight figures. The pennies (black "X") are easily visible since they are grouped together.

Analysis: This demonstrates that encryption preserves the data's relational architecture. The encrypted space retains the distances and relative locations that define the clustering in the original space. The enormous significant variance structures remain preserved after encryption, as evidenced by PCA's ability to produce separable projections.

Aspect 2: Effect of Normalization:
Observation: There are some minor but noticeable discrepancies between the normalized (Figures 2, 4, 5, and 7) and non-normalized (Figures 1, 3, 6) findings. Normalized clusters typically have a more geometric and compact appearance (Figure 2 vs. Figure 1, Figure 7 vs. Figure 6).
Analysis: Normalization helps to stabilize the encrypted distance measure. Despite having ciphertexts, features with higher original ranges may have a disproportionate impact on Euclidean distance even in the encrypted space, which is not normalized. Normalization prior to encryption eliminates this bias and produces more coherent clusters that show similar data rather than scale artifacts.
Aspect 3: K-Means++ Initialization Effectiveness:
Observation: The results obtained using K-Means++ (Figures 5, 6, 7) show a high cluster density and centroid placement. It is observed that the centroids are positioned in the middle of closely spaced, close-knit groupings.
Analysis: Unlike encrypted clustering, the method cannot naturally begin randomization using data magnitudes. By ensuring that the initial centroid sites are dispersed in a likely way, K-Means++ tackles the problem of improper initialization [16]. This prevents sub-optimal partitions, which is especially crucial in the opaque encrypted environment, and leads to faster convergence and more consistent results.
Aspect 4: Dimensionality (2D vs. 3D Visualization):
Observation: Figures 3, 4, 5, and 8 show cluster separation in an additional spatial dimension. This can occasionally highlight patterns that may be hidden in 2D (the ”bridging pattern of Cluster 3 in Figure 5 is easier to see in 3D).
Analysis: While 3D PCA can show a greater portion of the overall variance, 2D PCA can be utilized to demonstrate the concept of simple separability. This allows for a more thorough assessment of the boundary and overlap of clusters by providing a more realistic, if still distorted, representation of the geometry of the high-dimensional encrypted data.
Aspect 5: Privacy-Utility Trade-off:
Observation: Without disclosing the underlying features of the Iris dataset (sepal/petal lengths and widths), the visualizations offer some comprehensible cluster formations.
Evaluation: The pipeline successfully balances the trade-off between privacy and utility. It can be grouped using the effective operation of K-Means on ciphertexts, i.e., utility (cluster finding), and assisted geometric relations in the PCA space. Because the results of the analyses are encrypted (when computing is done) or are low-dimensional projections and cluster classifications that do not reveal sensitive initial values, privacy is guaranteed.

7.3. Sensitivity Analysis

Here, we address how sensitive the suggested privacy-preserving clustering system is to encrypted K-Means, K-Means++, PCA, homomorphic encryption, and feature normalization.
1. Normalization of Features:
Features are given equal weight in Euclidean distance (in encrypted space) thanks to normalization. Features with wide numerical ranges have a greater impact in the absence of normalization, which causes instability. Hulls are stable after normalization.
Conclusion: Scaling is very important.
2. Homomorphic:
Encryption: Although it limits precision and produces noise, encryption permits operations on encrypted data. In conclusion, encryption settings are (moderately) sensitive.
3. PCA:
PCA is a variance-preserving linear transformation. Structural information is lost when the number of components is reduced. In conclusion, the number of components has some influence.
4. Encrypted K-Means:
Initialization, approximation of the distance measure, and termination are necessary for the clustering.
Conclusion: quite susceptible to startup.
5. K-Means++:
Better centroid initialization and clustering instability.

Conclusion, it lessens sensitivity and stabilizes. In general, the main elements influencing stability are robustness and sensitivity.
Sensitivity analysis assesses how changes in methodological choices or factors affect the outcomes.
Sensitivity to Method of initializing:
Analysis: The system's sensitivity to centroid initialization can be determined by comparing the conventional K-Means and K-Means++. In normal K-Means with encrypted data, random seeding leads in inconsistent behavior on repeated executions (Figures 1, 3, 8), which may lead to unstable outputs. Such sensitivity is reduced by K-Means++ (Figures 5, 6, 7), which also produces stronger and more consistent clusterings. The encrypted domain, where the algorithm is unable to make heuristic readjustments based on plaintext values, further increases this sensitivity.
Normalization: Sensitivity to Pre-processing:
Analysis: The results' sensitivity depends on whether or not normalization is carried out. This is due to the fact that normalization changes the encrypted space's distance landscape as shown. Such sensitivity might rise much more in data sets with dissimilar feature scales (like the relatively scale-similar Iris features). In order to ensure that the encrypted clustering algorithm is used on a geometry that appropriately represents data similarity rather than arbitrary scaling, normalization is a crucial pre-processing step.
Dimensionality of PCA Projection Sensitivity:
Discussion: Analysis is the trade-off between interpretability and information loss in the 2D and 3D PCA projection alternatives. A highly interpretable 2D projection can obscure separation by squashing clusters, as seen in Figures 1, 2, 6, and 7. As seen in the discrete spatial volumes inhabited by clusters, a 3D projection (Figures 3, 4, 5, 8) can be more clearly distinguished and does not lose as much variance. This choice is system-sensitive; a 2D view may show better separation in higher dimensions, or vice versa.
Number of Clusters (k) Sensitivity:
Analysis: The Iris dataset uses the constant k=3, however the value of k is a parameter. Finding the ideal k in an encrypted environment is quite challenging (e.g. an encrypted elbow method or silhouette score). The system's outcomes have an impact on this user-defined parameter. The technique would split the encrypted data into an abnormal number of groups if k were incorrect, which would compromise the geometrical integrity of such visualizations.
Encryption Scheme parameters Sensitivity:
Analysis: Computational precision and noise increase are directly impacted by the parameters and HE methods (e.g., BGV, CKKS). We used CKKS in this study that approximate arithmetic, which may result in negligible errors when calculating distances. The visual uniformity between the pictures suggests that the scheme's chosen parameters were sufficient to guarantee numerical stability. However, the K-Means algorithm may become unstable at an iterative stage when a multiplicative depth or multiplicative precision is insufficient, leading to unsuccessful or meaningless clusters.

7.4. Conclusion of Analyses

The methodological, aspect-based, and sensitivity analysis approaches taken together demonstrate the strength and subtlety of the encrypted K-Means pipeline. Although its effectiveness depends on careful selection of normalization, initiation, and projection dimensions, it is effective in maintaining the geometry of data to cluster and ensure privacy. The visual results provide strong empirical evidence that the fundamental relationships in the data could be preserved during the data transfer to a secure, encrypted analytical domain.

8. Conclusion

This work has demonstrated that privacy-preserving clustering may be used on encrypted Iris data without requiring knowledge of the original feature values. Three significant clusters can be successfully identified in the encrypted space using Encrypted K-Means and Encrypted K-Means Plus, and PCA-based 2D and 3D projections demonstrate that centroid distinguishability and cluster separation are still visible in the encrypted space. By creating a much

narrower, more stable boundary that enables more dependable distance-based partitioning, feature normalization before encryption can further improve clustering dependability. Overall, the results indicate that encryption does not always destroy the data topology, and that appropriate preprocessing (normalization) and efficient initialization (K-Means++) may improve convergence stability and form preservation in the face of privacy constraints.

9. Limitations

Benchmark-scale data set weakness: Because the Iris dataset is small and well-structured, the findings may not be applicable to large-scale, noisy, high-dimensional real-world data where clustering behavior and encrypted distance calculations are more complex.
Interpretability based on visualization: Dimensionality reduction is likely to obscure small overlaps or inflate the actual distances between features in the original encrypted feature space, and the PCA-based projections employed to achieve interpretability are highly dependent on visualization.
Small metric coverage: Although the visual cluster separation is the main focus of the investigation, various quantitative validation techniques such as silhouette scores, Davies Bouldin index, or stability of indiscriminate initializations would improve the conclusions' rigor.
Limits in the encryption scheme not yet fully explored: The impact of different encryption or secure computation schemes on numerical accuracy of the result, distance computations, convergence behavior, and computational cost all of which can affect clustering fidelity in practice is not fully benchmarked in this paper.
Threat model scope: Although the raw feature values have been safeguarded, the analysis has not thoroughly examined the potential for information leakage due to data access patterns, encrypted intermediate output, or recurrence of query interactions in real-world settings.

Future Work:
Scale up Evaluation: Test robustness and applicability on bigger, more difficult data sets (high-dimensional, unbalanced, noisy, and sensitive to real-world data).
Broader validation metrics: PCA plots and quantitative cluster-quality/stability testing (multiple tests, sensitivity to seeding, robustness tests) are employed.
Compare secure methods: A shared experimental protocol must be used to compare privacy-preserving methods (such as trusted execution environments, safe multiparty computing, and homomorphic encryption variants).
Run time and cost profiling: ascertain the convergence time and compute overhead costs in order to clearly identify accuracy, privacy, and efficiency trade offs.
Extrapolate to further unsupervised issues: To scale privacy-compliant analytics, look at encrypted Gaussian mixtures, hierarchical clustering, DBSCAN-like, and encrypted dimensionality reduction.
Strong security analysis: In order to secure the pipeline in accordance with the realistic adversarial assumptions, build the threat model and assess the leakage points the pipeline can support.

Authors' Contributions: All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.
Competing Interests: The authors declare that they have no competing interests.

REFERENCES

1. F. Smarandache, *A unifying field in logics: Neutrosophic logic, neutrosophy, neutrosophic set, neutrosophic probability*, American Research Press, 1999. URL: https://fs.unm.edu/eBook-Neutrosophics6.pdf.
2. H. Wang, F. Smarandache, Y. Zhang, and R. Sunderraman, *Single Valued Neutrosophic Sets*, in Multispace & Multistructure. Neutrosophic Transdisciplinarity (100 Collected Papers of Sciences), vol. IV, edited by F. Smarandache, North-European Scientific Publishers, Hanko, Finland, pp. 410–413, 2010. URL: https://fs.unm.edu/SingleValuedNeutrosophicSets.pdf.
3. H. Wang, F. Smarandache, Y. Zhang, and R. Sunderraman, *Interval neutrosophic sets and logic: Theory and applications in computing*, 2005. DOI: 10.5555/1195136.

4. H. Zhang, J. Wang, and X. Chen, *Interval neutrosophic sets and their application in multicriteria decision making problems*, The Scientific World Journal, vol. 2014, 2014. DOI: 10.1155/2014/645953.
5. J. Ye, *A multicriteria decision-making method using aggregation operators for simplified neutrosophic sets*, Journal of Intelligent & Fuzzy Systems, vol. 26, no. 5, pp. 2459–2466, 2014. DOI: 10.3233/IFS-130916.
6. P. K. Maji, *Neutrosophic soft set*, Annals of Fuzzy Mathematics and Informatics, vol. 5, no. 1, pp. 157–168, 2013. URL: AFMI-5-1(157-168)-J-111216R1.pdf.
7. P. Biswas, S. Pramanik, and B. C. Giri, *Entropy-based grey relational analysis method for multi-attribute decision making under single valued neutrosophic assessments*, Neutrosophic Sets and Systems, vol. 2, pp. 102–110, 2014. DOI: 10.5281/zenodo.22459.
8. Y. Guo, and H. D. Cheng, *A new neutrosophic approach to image segmentation*, Pattern Recognition, vol. 42, no. 5, pp. 587–595, 2009. DOI: 10.1016/j.patcog.2008.10.002.
9. M. Zhang, L. Zhang, and H. D. Cheng, *A neutrosophic approach to image segmentation based on watershed method*, Signal Processing, vol. 91, no. 5, pp. 1260–1269, 2011. DOI: 10.1016/j.sigpro.2009.10.021.
10. S. Pramanik, and T. K. Roy, *Neutrosophic game theoretic approach to Indo–Pak conflict over Jammu–Kashmir*, Neutrosophic Sets and Systems, vol. 2, pp. 82–101, 2014. URL: https://fs.unm.edu/NSS/NeutrosophicGameTheoreticApproach.pdf.
11. A. C. Yao, *How to generate and exchange secrets*, in Proceedings of the 27th Annual Symposium on Foundations of Computer Science, pp. 162–167, 1986. DOI: 10.1109/SFCS.1986.25.
12. C. Gentry, *A fully homomorphic encryption scheme*, Doctoral dissertation, Stanford University, 2009. DOI: 10.13140/RG.2.2.31372.53129.
13. R. Bost, R. A. Popa, S. Tu, and S. Goldwasser, *Machine learning classification over encrypted data*, in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2015. URL: https://iot.stanford.edu/pubs/bost-learning-ndss15.pdf.
14. A. Jaschke, and F. Armknecht, *Accelerating homomorphic computations for machine learning on encrypted data*, in International Conference on Applied Cryptography and Network Security, 2016. DOI: 10.1007/978-3-319-39555-5_22.
15. V. Patel, D. Shah, and H. Sanghvi, *A review on privacy-preserving data mining using homomorphic encryption*, International Journal of Computer Applications, 2019.
16. D. Arthur, and S. Vassilvitskii, *k-means++: The advantages of careful seeding*, in Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 1027–1035, 2007. DOI: 10.1145/1283383.1283494.
17. P. Mohassel, P. Rindal, and M. Rosulek, *Fast database joins and PSI for secret shared data*, in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 2069–2086, 2020. DOI: 10.1145/3372297.3423358.
18. R. Hatamleh, *On the Form of Correlation Function for a Class of Nonstationary Field with a Zero Spectrum*, Rocky Mountain Journal of Mathematics, vol. 33, no. 1, pp. 159–173, 2003. DOI: 10.1216/rmjm/1181069991.
19. R. Hatamleh, and V. A. Zolotarev, *On Two-Dimensional Model Representations of One Class of Commuting Operators*, Ukrainian Mathematical Journal, vol. 66, no. 1, pp. 122–144, 2014. DOI: 10.1007/s11253-014-0916-9.
20. R. Hatamleh, and V. A. Zolotarev, *On Model Representations of Non-Selfadjoint Operators with Infinitely Dimensional Imaginary Component*, Journal of Mathematical Physics, Analysis, Geometry, vol. 11, no. 2, pp. 174–186, 2015. DOI: 10.15407/mag11.02.174.
21. R. Hatamleh, and V. A. Zolotarev, *Triangular Models of Commutative Systems of Linear Operators Close to Unitary Operators*, Ukrainian Mathematical Journal, vol. 68, no. 5, pp. 791–811, 2016. DOI: 10.1007/s11253-016-1258-6.
22. R. Hatamleh, and A. Hazaymeh, *On Some Topological Spaces Based On Symbolic n-Plithogenic Intervals*, International Journal of Neutrosophic Science, vol. 25, no. 1, pp. 23–37, 2025. DOI: 10.54216/IJNS.250102.
23. T. Qawasmeh, and R. Hatamleh, *A new contraction based on H-simulation functions in the frame of extended b-metric spaces and application*, International Journal of Electrical and Computer Engineering, vol. 13, no. 4, pp. 4212–4221, 2023. DOI: 10.11591/ijece.v13i4.pp4212-4221.
24. A. S. Heilat, H. Zureigat, R. Hatamleh, and B. Batiha, *New Spline Method for Solving Linear Two-Point Boundary Value Problems*, European Journal of Pure and Applied Mathematics, vol. 14, no. 4, pp. 1283–1294, 2021. DOI: 10.29020/nybg.ejpam.v14i4.4124.
25. M. Ali, and F. Smarandache, *Complex Neutrosophic Set*, Neural Computing and Applications, vol. 25, pp. 1–18, 2016. DOI: 10.1007/S00521-015-2154-Y.
26. H. Qawaqneh, *Fractional Analytic Solutions and Fixed Point Results with Some Applications*, Advances in Fixed Point Theory, vol. 14, article 1, 2024. DOI: 10.28919/afpt/8279.
27. H. Qawaqneh, M. S. M. Noorani, H. Aydi, A. Zraiqat, and A. H. Ansari, *On Fixed Point Results in Partial b-Metric Spaces*, Journal of Function Spaces, vol. 2021, Article ID 8769190, 2021. DOI: 10.1155/2021/8769190.
28. H. Qawaqneh, M. S. M. Noorani, and H. Aydi, *Some New Characterizations and Results for Fuzzy Contractions in Fuzzy B-Metric Spaces and Applications*, AIMS Mathematics, vol. 8, pp. 6682–6696, 2023. DOI: 10.3934/math.2023338.
29. H. Qawaqneh, J. Manafian, M. Alharthi, and Y. Alrashedi, *Stability Analysis, Modulation Instability, and Beta-Time Fractional Exact Soliton Solutions to the Van Der Waals Equation*, Mathematics, vol. 12, article 2257, 2024. DOI: 10.3390/math12142257.
30. H. Qawaqneh, *New Functions for Fixed Point Results in Metric Spaces with Some Applications*, Indian Journal of Mathematics, vol. 66, pp. 55–84, 2024.
31. H. Qawaqneh, H. A. Hammad, and H. Aydi, *Exploring New Geometric Contraction Mappings and Their Applications in Fractional Metric Spaces*, AIMS Mathematics, vol. 9, pp. 521–541, 2024. DOI: 10.3934/math.2024028.
32. M. Elbes, T. Kanan, M. Alia, and M. Ziad, *Covd-19 Detection Platform from X-Ray Images Using Deep Learning*, International Journal of Advanced Soft Computing Applications, vol. 14, pp. 197–211, 2022. DOI: 10.15849/ijasca.220328.13.
33. T. Kanan, M. Elbes, K. A. Maria, and M. Alia, *Exploring the Potential of IoT-Based Learning Environments in Education*, International Journal of Advanced Soft Computing Applications, vol. 15, pp. 166–178, 2023.