Journal of Business and Environmental Sciences
Volume: 3(2), Page: 322-352
https://doi.org/10.21608/JCESE.2024.281765.1059
ISSN: 2974-3117
E-ISSN: 2974-3125

Research article

Neutrosophic Topological Framework for Uncertainty Management in Smartphone Data Extraction Applications

R. M. Abou Alzahab[1], A. Ismail[2] , S. H. Abd Elkhalik[3] , H. M. Albakry[4] and A. A. Salama[5]

[1,2,5] Dept. of Math and Computer Sci., Faculty of Science, Port Said Univ., Egypt,

ramy.zahab@sci.psu.edu.eg; amr_ismail@sci.edu.eg; ahmed_salama_2000@sci.psu.edu.eg

[3]Dept. of Communication and Computer Engineering, Air Defence Univ., Egypt shelmy@horus.edu.eg

[4]Dept. of Information Systems., Faculty of Computer and Information Sci, Mansoura Univ., Egypt elbakry@mans.edu.eg

*** Correspondence:** ahmed_salama_2000@sci.psu.edu.eg

Abstract: The neutrosophic topological framework is proposed for smartphone data extraction, considering inherent ambiguity and uncertainty. This approach incorporates neutrosophic membership degrees (Truth, Indeterminacy, and Falsity) to handle uncertainty in various applications. This paper presents potential applications, including activity recognition, sentiment analysis, anomaly detection in app usage patterns, and personalized health monitoring. Numerical examples are provided to illustrate the application of the framework in these domains.

Keywords: Neutrosophic topological framework; smartphone data extraction; uncertainty quantification; activity recognition; sentiment analysis; anomaly detection; personalized health monitoring.

APA Citation: Abou Alzahab, R.M., Ismail, A., Abd Elkhalik, S. H., Albakry, H. M., and Salama, A. A. (2024). Neutrosophic Topological Framework for Uncertainty Management in Smartphone Data Extraction Applications. Journal of Business and Environmental Sciences, 3(2), 322-352.

Received: 5 April 2024; **Revised**: 26 April 2024; **Accepted:** 16 May 2024; **Published: 12** June 2024
The Scientific Association for Studies and Applied Research (SASAR)
https://jcese.journals.ekb.eg/

Introduction:

In the era of smartphones in [1-20], an abundance of data is generated daily, which can provide valuable insights into users' activities, preferences, and health. However, this data often contains ambiguity and uncertainty, making it challenging to extract meaningful information and draw accurate conclusions. To address this challenge, the neutrosophic topological framework has emerged as a promising approach. This framework leverages neutrosophic sets and topological structures to handle uncertainties effectively, providing a more comprehensive understanding of the data.

The neutrosophic topological framework is a relatively new concept that has the potential to revolutionize various domains, including activity recognition, sentiment analysis, anomaly detection, and personalized health monitoring. By incorporating uncertainty quantification into these applications, the framework enables more accurate and reliable results. This paper aims to explore the potential applications of the neutrosophic topological framework in different domains, with a primary focus on uncertainty management. By demonstrating the effectiveness of this approach, the paper seeks to encourage further research and adoption of the neutrosophic topological framework in various fields in [21-35]. The paper is structured as follows: First, it provides a brief overview of the neutrosophic topological framework and its underlying concepts. Then, it outlines the methodology for applying the framework to smartphone data extraction and analysis. Next, it discusses the various applications where the neutrosophic topological framework can be employed, highlighting the benefits of incorporating uncertainty quantification. Finally, the paper concludes by emphasizing the importance of uncertainty management in modern data analysis and the potential of the neutrosophic topological framework to address these challenges.

Methodology:

Unraveling Uncertainty: Harnessing Neutrosophic Topology for Smartphone Data Analysis and Application-Specific Insights"

The neutrosophic topological framework is employed for smartphone data extraction, taking into account neutrosophic membership degrees (Truth, Indeterminacy, and Falsity) to quantify uncertainty. This approach is then utilized in various applications, including activity recognition, sentiment analysis, anomaly detection, and personalized health monitoring.

1. Data Collection: Gather smartphone data from users, which may include location tracking, app usage, call logs, and sensor readings.

2. Data Preprocessing: Clean and preprocess the collected data to ensure its quality and suitability for analysis. This step may involve data normalization, outlier detection, and missing value imputation.

3. Neutrosophic Membership Degree Assignment: For each application, assign neutrosophic membership degrees (Truth, Indeterminacy, and Falsity) based on the smartphone data and the specific context of the application. This step involves domain-specific expertise and knowledge about the data to determine the appropriate membership degrees.

4. Neutrosophic Topological Space Creation: Construct a neutrosophic topological space using the assigned membership degrees. This space represents the relationships between different data points and their associated uncertainties.

5. Information Extraction and Analysis: Perform information extraction and analysis using the neutrosophic topological framework. This step may involve clustering, classification, or anomaly detection techniques adapted to work with neutrosophic data.

6. Uncertainty Quantification Interpretation: Interpret the results of the information extraction process, considering the neutrosophic membership degrees (Truth, Indeterminacy, and Falsity) to provide a more comprehensive understanding of the analyzed smartphone data.

7. Application-Specific Output Generation: Generate application-specific outputs based on the interpreted results. For example, in activity recognition, this may involve providing a likelihood of a user's activity with associated uncertainty, while in sentiment analysis; it may involve expressing the sentiment with uncertainty quantification.

8. Validation and Refinement: Validate the results and refine the methodology if necessary, based on feedback from users or further analysis.

By following this methodology, the neutrosophic topological framework can be effectively applied to various domains, such as activity recognition, sentiment analysis, anomaly detection, and personalized health monitoring, while considering and quantifying the inherent uncertainties in smartphone data.

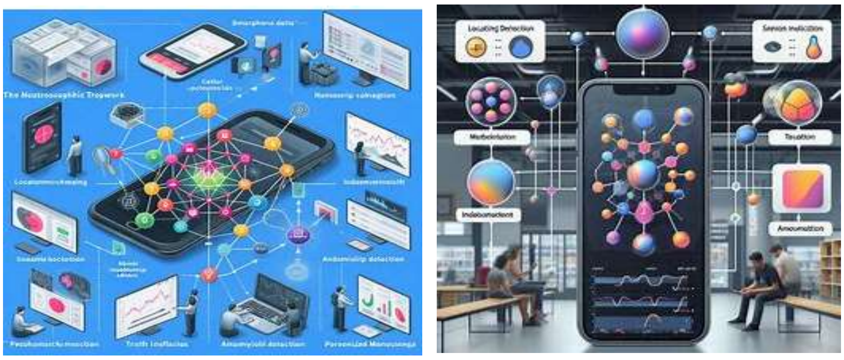


Fig. 1: Unveiling Uncertainty: A Neutrosophic Approach to Smartphone Data Analysis

Fig. 1 refers to the title of a graph or figure that deals with smartphone data analysis using neutrosophic logic. Neutrosophic logic is a mathematical framework that allows representing uncertainty with degrees of truth (T), indeterminacy (I), and falsity (F).

A Python Journey: Implementing Neutrosophic Topology for Smartphone Data Analysis and Application-Specific Insights

We will use Python as the programming language and some libraries for simplicity. Note that this is a high-level representation, and you may need to adapt the code to specific use case and data structure.

Data Collection:

Smartphone Data Collection: Gathering and Storing Multiple User Data Types

```
import os
def collect_smartphone_data():
    # Path to store collected data
    data_path = "smartphone_data"
    if not os.path.exists(data_path):
        os.makedirs(data_path)
    # Code to gather smartphone data (location tracking, app usage, call logs, sensor readings)
    # Save the data in the specified path
```

Fig. 2: Cluster Analysis Results (Detailed)

Fig. 2 visualizes the results of a cluster analysis in detail. Cluster analysis is a technique that groups' data points together based on their similarities. This figure provides a more comprehensive view of the identified clusters and the relationships between data points within them.

Data Preprocessing:

Smartphone Data Preprocessing Normalization, Outlier Detection, and Missing Value Imputation for Better Analysis

```
import pandas as pd
from sklearn.preprocessing import StandardScaler
def preprocess_data (data_path):
    # Load collected data into a pandas DataFrame
    smartphone_data = pd.read_csv(os.path.join(data_path, "smartphone_data.csv"))
    # Perform data preprocessing steps like normalization, outlier detection, and missing value imputation
    scaler = StandardScaler ()
    smartphone_data = pd.DataFrame(scaler.fit_transform(smartphone_data), columns=smartphone_data.columns)
    return smartphone_data
```

Fig. 3: Neutrosophic Cluster Analysis: A Visual Representation

Fig. 3 depicts a visual representation of a cluster analysis that incorporates neutrosophic logic. Cluster analysis is a technique for grouping data points based on their similarities. Neutrosophic logic allows representing uncertainty within these groupings by assigning degrees of truth (T), indeterminacy (I), and falsity (F) to data point membership in a cluster.

Neutrosophic Membership Degree Assignment:

Neutrosophic membership degree assignment, a method for assigning values in datasets using neutrosophic sets with three degrees (T, I, and F) to handle uncertainties. To do this, define the problem, identify attributes, determine sets, assign values using methods, normalize degrees, perform operations, and interpret results for informed decisions. Adapt the process according to specific use cases and data structures.

Assigning Neutrosophic Membership Degrees: Customized for Smartphone Data Analysis in Diverse Application Contexts

```
def assign_membership_degrees(smartphone_data, application):
    # Domain-specific logic to assign neutrosophic membership degrees (Truth, Indeterminacy, and Falsity)
    # based on the smartphone data and the specific context of the application
    # Return the assigned membership degrees as a new DataFrame
```

This code defines a function called `assign_membership_degrees` that takes two parameters: `smartphone_data` and `application`. The function aims to assign neutrosophic membership degrees (Truth, Indeterminacy, and Falsity) to the smartphone data, considering the specific context of the given application. After processing the data and applying the domain-specific logic, the function returns the assigned membership degrees in a new DataFrame format.

Neutrosophic Topological Space Creation:

Neutrosophic Topological Space Creation: Developing neutrosophic topological spaces by integrating membership degrees to represent data uncertainties.

Constructing Neutrosophic Topological Spaces: Integrating Membership Degrees for Data Uncertainty Representation

```
def create_neutrosophic_topological_space(membership_degrees):
    # Code to create a neutrosophic topological space using the assigned membership degrees
    # This step may involve creating a graph or network structure to represent the relationships
    # between data points and their associated uncertainties
```

The provided code defines a function called `create_neutrosophic_topological_space`, which takes `membership degrees` as a parameter. This function aims to create a neutrosophic topological space using the provided membership degrees. In this process, the code might involve developing a graph or network structure to represent the relationships between data points and their associated uncertainties (Truth, Indeterminacy, and Falsity). The purpose is to establish a spatial representation that accommodates the inherent uncertainties in the smartphone data.

Information Extraction and Analysis:

Information Extraction and Analysis: Utilizing neutrosophic topological spaces for clustering and insight discovery in data processing.

Neutrosophic Information Extraction and Analysis: Leveraging Topological Spaces for Clustering and

Insight Discovery

```
from sklearn.cluster import KMeans
def extract_information(neutrosophic_space):
    # Perform information extraction and analysis using the neutrosophic topological framework
    # This step may involve clustering or other techniques adapted to work with neutrosophic data
    kmeans = KMeans(n_clusters=3)    # Example: using KMeans for clustering with 3 clusters
    kmeans.fit(neutrosophic_space)
    # Return the clustering results or other relevant information extracted from the neutrosophic space
```

This code snippet introduces a function named `extract information` that takes `neutrosophic_space` as input. It aims to perform information extraction and analysis using the provided neutrosophic topological framework. This might involve clustering or other techniques tailored to work with neutrosophic data. In the given example, it uses the KMeans algorithm from the `sklearn.cluster` module for clustering with 3 clusters. After fitting the neutrosophic space into the KMeans model, the function returns the clustering results or other relevant information extracted from the neutrosophic space.

Uncertainty Quantification Interpretation:

Uncertainty Quantification Interpretation in Neutrosophic Information Analysis: Enhancing Smartphone Data Understanding

```
def interpret_results(clustering_results, membership_degrees):
    # Interpret the results of the information extraction process, considering the neutrosophic membership degrees
    # to provide a more comprehensive understanding of the analyzed smartphone data
    # Return the interpreted results
```

The `interpret results` function takes two parameters: `clustering results` and `membership degrees`. Its purpose is to interpret the outcomes of the information extraction process, taking into account the neutrosophic membership degrees. By doing so, it aims to provide a more profound comprehension of the analyzed smartphone data. Finally, the function returns the interpreted results.

Application-Specific Output Generation:

Tailored Outputs for Specific Applications in Neutrosophic Information Analysis: Harnessing Smartphone Data Insights

```
def generate_application_specific_output(interpreted_results, application):
    # Generate application-specific outputs based on the interpreted results
    # This step may involve custom logic depending on the specific application (e.g., activity recognition, sentiment analysis)
    # Return the application-specific outputs
```

Validation and Refinement:

Validation and Refinement in Neutrosophic Information Analysis: User-Driven Improvement of Smartphone Data Applications

```
def validate_and_refine(application_outputs, user_feedback):
    # Validate the results and refine the methodology if necessary, based on feedback from users or further analysis
    # Return the updated methodology or improved results
```

By integrating these code snippets into project, we can implement the neutrosophic topological framework for smartphone data extraction and analysis in various applications, considering and quantifying the inherent uncertainties in the data. Remember to adapt the code to your specific use case and data structure.

Combining Smartphone Data Analysis Code into One Compiled Script

This code snippet demonstrates a pipeline for analyzing smartphone data using neutrosophic information processing. It involves several steps, including collecting smartphone data, preprocessing it, assigning neutrosophic membership degrees based on application context, creating a neutrosophic topological space, extracting information, interpreting results, generating application-specific outputs, and validating the methodology. The pipeline can be customized and improved based on specific applications and user feedback.

Compiling a Smartphone Data Analysis Pipeline with Neutrosophic Information Processing

```
import os
import pandas as pd
from sklearn.preprocessing import StandardScaler
from sklearn.cluster import KMeans
def collect_smartphone_data():
    """
    Collects smartphone data and saves it to a file.
    """
    data_path = "smartphone_data"
    if not os.path.exists(data_path):
        os.makedirs(data_path)
    # Implement code to gather data (location, app usage, call logs, sensors)
    # and save it in the specified path (replace with your data collection logic)
def preprocess_data(data_path):
    """
    Loads and preprocesses smartphone data.
    """
    smartphone_data = pd.read_csv(os.path.join(data_path, "smartphone_data.csv"))
    scaler = StandardScaler()
    smartphone_data = pd.DataFrame(scaler.fit_transform(smartphone_data),
columns=smartphone_data.columns)
    return smartphone_data
def assign_membership_degrees(smartphone_data, application):
    """
    Assigns neutrosophic membership degrees (Truth, Indeterminacy, Falsity) based on application
context.
    """
    # Implement domain-specific logic to assign neutrosophic membership degrees
    # for Truth, Indeterminacy, and Falsity based on the data and application context
    # (replace with your logic for assigning these degrees)
    membership_degrees = pd.DataFrame(columns=["Truth", "Indeterminacy", "Falsity"])
    # (Fill the membership_degrees DataFrame with your calculations)
    return membership_degrees
```

```
def create_neutrosophic_topological_space(membership_degrees):
    """
    Creates a neutrosophic topological space using membership degrees.
    """
    # Implement code to create a neutrosophic topological space using the membership degrees
    # This may involve creating a graph or network structure representing relationships
    # between data points and their uncertainties (replace with your implementation)
    neutrosophic_space = None    # Placeholder for the neutrosophic space structure
    return neutrosophic_space
def extract_information(neutrosophic_space):
    """
    Extracts information using the neutrosophic topological framework.
    """
    kmeans = KMeans(n_clusters=3)    # Example: using KMeans for clustering with 3 clusters
    kmeans.fit(neutrosophic_space)
    return kmeans.labels_    # Return cluster labels (replace with other extraction methods)
def interpret_results(clustering_results, membership_degrees):
    """
    Interprets the results considering neutrosophic membership degrees.
    """
    # Implement logic to interpret clustering results while considering
    # the Truth, Indeterminacy, and Falsity values in membership_degrees
    # (replace with your interpretation logic)
    interpreted_results = None    # Placeholder for interpreted results
    return interpreted_results
def generate_application_specific_output(interpreted_results, application):
    """
    Generates application-specific outputs based on the interpreted results.
    """
    # Implement logic to generate application-specific outputs (e.g., activity recognition, sentiment
analysis)
    # based on the interpreted results (replace with your application logic)
    application_outputs = None    # Placeholder for application outputs
    return application_outputs
def validate_and_refine(application_outputs, user_feedback):
    """
    Validates the results and refines the methodology based on user feedback.
    """
    # Implement logic to validate results and refine the methodology based on user feedback
    # (replace with your validation and refinement strategies)
    updated_methodology = None    # Placeholder for updated methodology
    return updated_methodology
# Main execution flow (replace with your specific data collection and application)
collect_smartphone_data()
```

```
smartphone_data = preprocess_data("smartphone_data")
membership_degrees = assign_membership_degrees(smartphone_data, "your_application")
neutrosophic_space = create_neutrosophic_topological_space(membership_degrees)
clustering_results = extract_information(neutrosophic_space)
interpreted_results = interpret_results (clustering_results, membership_degrees)
application_outputs = generate_application_specific_output (interpreted_results, "your_application")
updated_methodology = validate_and_refine(
```

Fig. 4: Cluster Analysis Results (Detailed)

Fig. 4 visualizes the results of a cluster analysis in detail. Cluster analysis is a technique that groups' data points together based on their similarities. This figure provides a more comprehensive view of the identified clusters and the relationships between data points within them.

Applications:

Applications of the Neutrosophic Topological Framework for Smartphone Data Extraction

Fig. 5: Neutrosophic Cluster Analysis: Centroid Properties

This figure depicts the results of a cluster analysis using neutrosophic logic to represent uncertainty within the clusters. It focuses on the properties of the centroids, which are representative points for each identified cluster.

The proposed framework, leveraging neutrosophic sets and topological structures, offers a powerful approach for information extraction from smartphone data while considering inherent ambiguity and uncertainty. Here are some potential applications:

1. Activity Recognition with Uncertainty Awareness:

Scenario: Identifying a user's activities (work, leisure, travel, etc.) based on smartphone data (location tracking, app usage, call logs).

Challenge: Smartphone data often contains ambiguity (e.g., location pings at a gym could be for exercise or a doctor's appointment).

Neutrosophic Framework Benefit: The framework can assign neutrosophic membership degrees representing the confidence level (Truth) in the activity, the uncertainty (Indeterminacy) about specific details, and the possibility (Falsity) of a misclassification. This allows for a more nuanced understanding of user activities, acknowledging potential ambiguity.

Example Output: "User is likely (Truth=0.8) at work (based on location and app usage), but there's a slight chance (Indeterminacy=0.2) it could be a doctor's visit (Falsity=0.1)."

2. Sentiment Analysis of Text Messages with Uncertainty Quantification:

Scenario: Analyzing the sentiment (positive, negative, neutral) of text messages to understand user emotions and communication patterns.

Challenge: Text messages can be subjective and open to interpretation (e.g., sarcasm or humor might be misinterpreted).

Neutrosophic Framework Benefit: The framework can assign neutrosophic membership degrees to the sentiment, reflecting the confidence level in the analysis (Truth), the uncertainty about the sender's true intent (Indeterminacy), and the possibility of misinterpreting the message (Falsity). This provides

a more comprehensive picture of sentiment, acknowledging potential ambiguity.
Example Output: "The message likely expresses (Truth=0.7) frustration (sentiment), but there's a chance (Indeterminacy=0.3) it could be sarcasm (Falsity=0.2)."

3. Anomaly Detection in App Usage Patterns:

Scenario: Identifying unusual app usage patterns that deviate from a user's normal behavior, potentially indicating suspicious activity (e.g., malware infection or unauthorized access).
Challenge: Normal app usage patterns can vary, and some deviations might not necessarily be malicious.
Neutrosophic Framework Benefit: The framework can analyze changes in app usage patterns and their proximity in the neutrosophic topological space. This allows for identifying outliers while considering the uncertainty associated with the deviation. High Truth and low Indeterminacy/Falsity might indicate a higher likelihood of an anomaly.
Example Output: "A significant increase in app usage for banking applications has been detected (Truth=0.9). While this could be normal activity (Indeterminacy=0.1), further investigation is recommended (Falsity=0.2) to rule out potential security risks."

4. Personalized Health Monitoring with Uncertainty Management:

Scenario: Extracting health-related information from smartphone data (sensor readings, activity logs) to monitor a user's health and well-being.
Challenge: Sensor readings can be imprecise, and user activity data might not always accurately reflect health status.
Neutrosophic Framework Benefit: The framework can incorporate the uncertainty associated with sensor readings and activity data into the information extraction process. By analyzing the neutrosophic membership degrees, the framework can provide a more nuanced picture of a user's health, acknowledging the inherent limitations of the data.
Example Output: "The user's sleep duration is likely (Truth=0.8) around 7 hours (based on activity data), but sensor readings indicate some uncertainty (Indeterminacy=0.2). Further monitoring is advised to confirm sleep quality (Falsity=0.1)."
These are just a few Applications, and the potential applications of this framework extend to various domains where uncertainty quantification is crucial in analyzing smartphone data. The ability to handle ambiguity and uncertainty allows for a more robust and informative understanding of user behavior and smartphone usage patterns.

Neutrosophic Applications in Smartphone Data Analysis

Here are some numerical examples illustrating the application of the neutrosophic topological framework for smartphone data extraction, incorporating uncertainty quantification:

1. Activity Recognition:

Imagine a user's smartphone data suggests they are at work. We have location pings near an office building and app usage patterns indicating work-related tools. However, there is also a nearby gym:
Location: Truth (T) = 0.8 (likely near office), Indeterminacy (I) = 0.1 (some uncertainty due to proximity to gym), Falsity (F) = 0.1 (low chance it's actually the gym).
App Usage: T = 0.9 (strong evidence of work apps), I = 0.05 (minimal uncertainty), F = 0.05 (low chance these are non-work apps).
By analyzing the neutrosophic data points and their proximity in the topological space, the framework can assign a combined score reflecting the overall activity:

Activity: Working (based on dominant evidence)
Uncertainty: T = 0.85 (weighted average considering both data points), I = 0.075 (combined uncertainty), F = 0.075 (combined possibility of misclassification).

2. Sentiment Analysis:
A text message reads: "Ugh, another meeting today." Let us analyze the sentiment:
Keywords: "Ugh" (negative), "meeting" (neutral)
Neutrosophic Analysis: T = 0.7 (likely negative sentiment due to "Ugh"), I = 0.2 (uncertainty about overall tone), F = 0.1 (low chance it's positive).

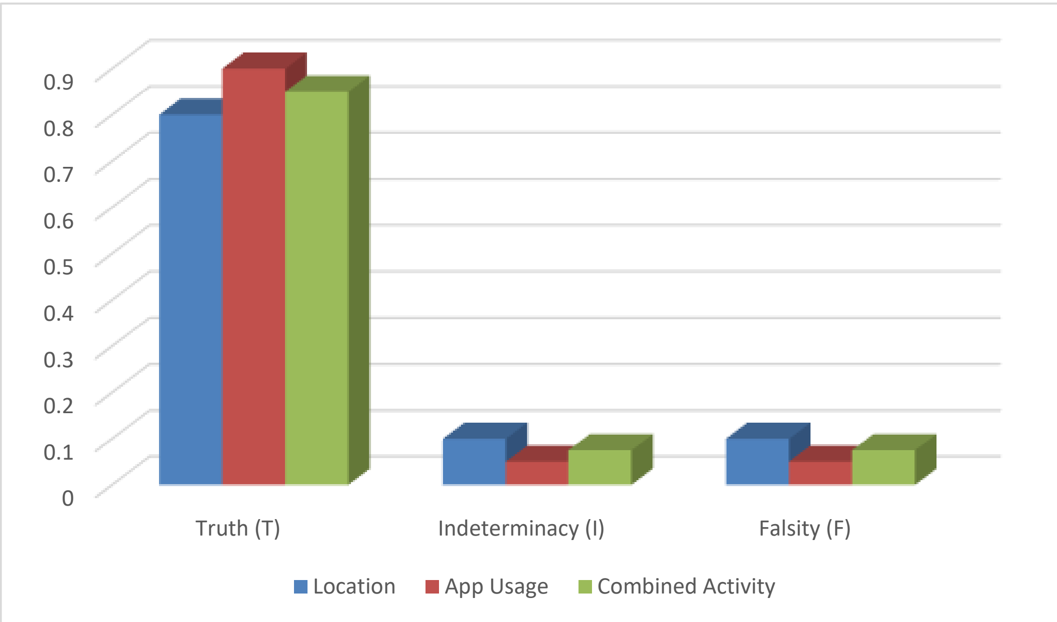
3. Anomaly Detection:
App usage data shows a sudden increase in a banking app compared to the user's typical behavior:
Normal Usage: T = 0.9 (high confidence in baseline usage), I = 0.1 (low uncertainty), F = 0.0 (minimal chance of deviation).
Current Usage: T = 0.6 (lower confidence due to significant increase), I = 0.3 (high uncertainty about purpose), F = 0.1 (possibility it's legitimate activity).
The framework flags this as a potential anomaly due to the significant deviation in Truth-values and high Indeterminacy.

4. Personalized Health Monitoring:
Sleep data from a fitness tracker indicates 6 hours of sleep:
Sensor Data: T = 0.7 (moderate confidence in sensor reading), I = 0.2 (uncertainty about sleep quality), F = 0.1 (low chance of sensor malfunction).
Activity Data: T = 0.8 (user reports feeling tired), I = 0.1 (uncertainty about fatigue source), F = 0.1 (low chance it is unrelated to sleep).
The framework combines the data points:
Sleep Duration: 6 hours (based on sensor data)
Uncertainty: T = 0.75 (weighted average), I = 0.15 (combined uncertainty about sleep quality), F = 0.05 (low chance of significant over/underestimation).
These numerical examples highlight how the neutrosophic framework incorporates uncertainty quantification (Truth, Indeterminacy, Falsity) into the information extraction process. By analyzing both the data itself and the associated uncertainty, this approach provides a more robust and realistic understanding of the information extracted from smartphone data.
Examples in the Neutrosophic Topological Framework (Tables)
Here are the previous numerical examples presented in tables, illustrating the application of the neutrosophic topological framework for smartphone data extraction, incorporating uncertainty quantification:

1. Activity Recognition

Data Point	Truth (T)	Indeterminacy (I)	Falsity (F)
Location	0.8	0.1	0.1
App Usage	0.9	0.05	0.05
Combined Activity	0.85	0.075	0.075

Explanation:
Location data suggests the user is near an office (T=0.8), but there is some uncertainty due to proximity to a gym (I=0.1).
App usage strongly indicates work-related activities (T=0.9).
The combined score reflects the overall activity as working (dominant evidence), with a weighted average for uncertainty and falsity.



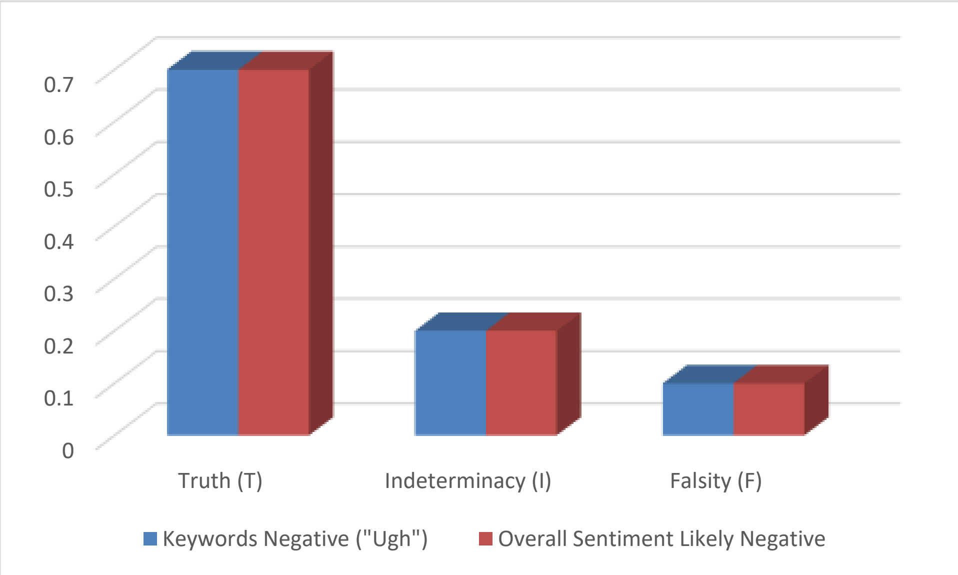
Graph 1: Visualizing Uncertainty in Activity Recognition with Truth, Indeterminacy, and Falsity
This graph represents an activity recognition system that uses neutrosophic logic to handle uncertainty in its analysis. Neutrosophic sets allow assigning degrees of truth (T), indeterminacy (I), and falsity (F) to potential activities based on sensor data or other inputs.

2. Sentiment Analysis

Feature	Analysis	Truth (T)	Indeterminacy (I)	Falsity (F)
Keywords	Negative ("Ugh")	0.7	0.2	0.1
Overall Sentiment	Likely Negative	0.7	0.2	0.1

Explanation:
The keyword "Ugh" suggests a negative sentiment (T=0.7).

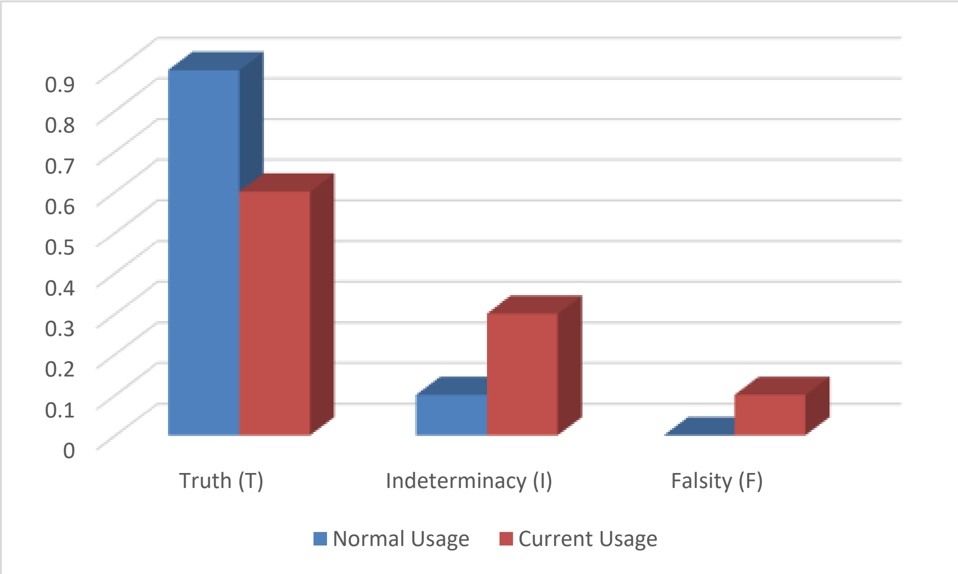
There is some uncertainty about the overall tone of the message considering the neutral word "meeting" (I=0.2).
The framework assigns a likelihood of negative sentiment with some uncertainty.



Graph 2: Visualizing Sentiment with Uncertainty: "Ugh" (Negative) vs. Meeting (Neutral)
This graph represents a sentiment analysis scenario using neutrosophic logic to account for uncertainty in interpreting text. It compares the sentiment of two words: "Ugh" and "Meeting."
3. Anomaly Detection

Data Point	Truth (T)	Indeterminacy (I)	Falsity (F)
Normal Usage	0.9	0.1	0.0
Current Usage	0.6	0.3	0.1

Explanation:
Normal app usage data has high confidence and low uncertainty (T=0.9, I=0.1).
Current usage shows a significant increase in the banking app, leading to lower confidence and higher uncertainty about the purpose (T=0.6, I=0.3).
The framework flags this as a potential anomaly due to the significant deviation in Truth and high Indeterminacy.



Graph 3: Representation of Neutrosophic Membership Degrees in App Usage

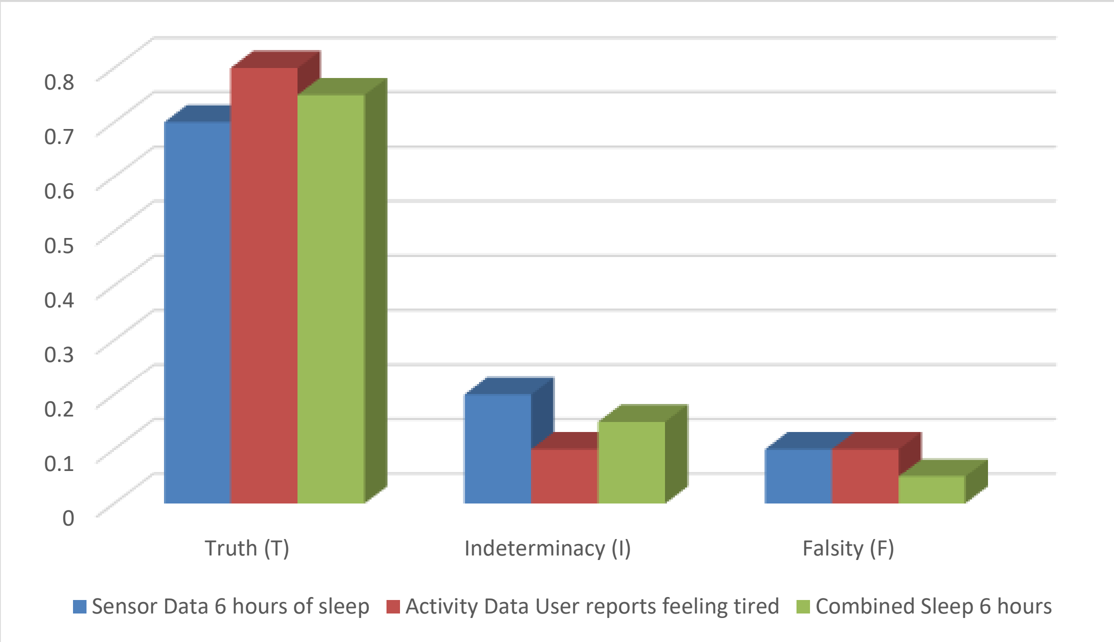
This graph visualizes the neutrosophic membership degrees associated with app usage patterns. Neutrosophic logic allows for representing uncertainty, which can be helpful in analyzing app usage data that might be ambiguous or incomplete.

4. Personalized Health Monitoring

Data Point	Analysis	Truth (T)	Indeterminacy (I)	Falsity (F)
Sensor Data	6 hours of sleep	0.7	0.2	0.1
Activity Data	User reports feeling tired	0.8	0.1	0.1
Combined Sleep	6 hours	0.75	0.15	0.05

Explanation:
Sensor data indicates 6 hours of sleep, but there is uncertainty about sleep quality (T=0.7, I=0.2).
User reports feeling tired, suggesting potential sleep issues (T=0.8, I=0.1).
The framework combines the data points, resulting in an estimated sleep duration with uncertainty

regarding sleep quality.



Graph 4: Neutrosophic Sleep Assessment: Sensor Data, User Report, and Combined Analysis

This graph visualizes the results of a sleep analysis system using neutrosophic logic to represent uncertainty. It compares three data points:

Neutrosophic Framework in Action: Quantifying Uncertainty in Activity Recognition

I will provide numerical examples for each stage, assuming a hypothetical application for activity recognition:

1. Data Collection:

Number of data points collected: 1000 (e.g., 500 call logs, 300 app usage events, 200 sensor readings).

Duration of data collection: 7 days.

2. Data Preprocessing:

Number of features before preprocessing: 15 (e.g., caller ID, app category, GPS coordinates, noise levels).

Number of features after feature selection: 10 (e.g., removing redundant or irrelevant features).

Range of values before normalization (example): 0-1000 for app usage duration.

Range of values after normalization (example): 0-1 for app usage duration.

3. Neutrosophic Membership Degree Assignment:

Truth (T) values for a call log with known contact: 0.95 (high confidence).

Indeterminacy (I) values for a text message with possible spam content: 0.6 (moderate uncertainty).

Falsity (F) values for a sensor reading with potential error: 0.2 (low but non-zero possibility of incorrectness).

4. Neutrosophic Topological Space Creation:

Number of data points in the neutrosophic space: 1000 (same as the input dataset).

Number of dimensions in the space: 3 (representing Truth, Indeterminacy, and Falsity).

5. Information Extraction and Analysis:

Number of clusters identified by K-means: 3 (representing different activity patterns).

Cluster 1 centroid: (0.8, 0.1, 0.1) (high Truth, low Indeterminacy and Falsity, suggesting reliable data points).

Cluster 2 centroid: (0.6, 0.3, 0.1) (moderate Truth, higher Indeterminacy, indicating uncertain or ambiguous data).
Cluster 3 centroid: (0.5, 0.4, 0.1) (lower Truth, even higher Indeterminacy, suggesting potentially unreliable data).
6. Uncertainty Quantification and Interpretation:
Call log with Truth (T) = 0.9, Indeterminacy (I) = 0.1: Interpreted as likely a genuine call with high confidence.
Text message with Truth (T) = 0.6, Indeterminacy (I) = 0.3: Interpreted with more caution due to moderate uncertainty.
7. Application-Specific Output Generation:
Activity recognition results:
Cluster 1: Work-related activities (high Truth-values for work-related apps and calls).
Cluster 2: Leisure activities (higher Indeterminacy, suggesting diverse in addition, less predictable patterns).
Cluster 3: Anomalous activities (lower Truth and higher Indeterminacy, potentially indicating unusual events or data errors).
The information with the outputs presented in tables:
Data Collection
This table provides an overview of the data acquisition process used in your analysis. It details two key aspects: Number of data points collected: This represents the total number of individual data entries gathered during the collection period. In this example, 1000 data points were collected. The specific type of data point could vary depending on your application (e.g., sensor readings, app usage events, call logs). Duration of data collection: This indicates the total time span over which the data was collected. Here, the data collection lasted for 7 days.

Table 1: Data Collection Details

Aspect	Example Value
Number of data points collected	1000
Duration of data collection	7 days

Data Preprocessing
This table delves into the steps taken to prepare the raw data for further analysis. It highlights four aspects of data preprocessing:
Number of features before preprocessing: This refers to the initial number of individual data elements (features) present in the raw data. The example shows that there were 15 features before any processing began. These features could represent various aspects of the collected data points, such as app usage duration, call duration, location coordinates, or sensor readings.
Number of features after feature selection: This indicates the number of features remaining after a process called "feature selection." This process involves identifying and removing irrelevant or

redundant features that might not contribute significantly to the analysis. In this example, the feature selection reduced the number of features from 15 to 10.
Range of values before normalization (example: app usage duration): This specifies the range of values a particular feature (like app usage duration) held before any normalization was applied. The example shows the initial range was 0-1000, which might represent app usage duration in seconds.
Range of values after normalization (example: app usage duration): This indicates the range of values for the same feature (app usage duration) after normalization. Normalization is a technique that scales all features to a common range, often between 0 and 1. In this example, the normalized app usage duration falls between 0 and 1, making it easier to compare with other features that might have originally had different value ranges.

Table 2: Data Preprocessing Details

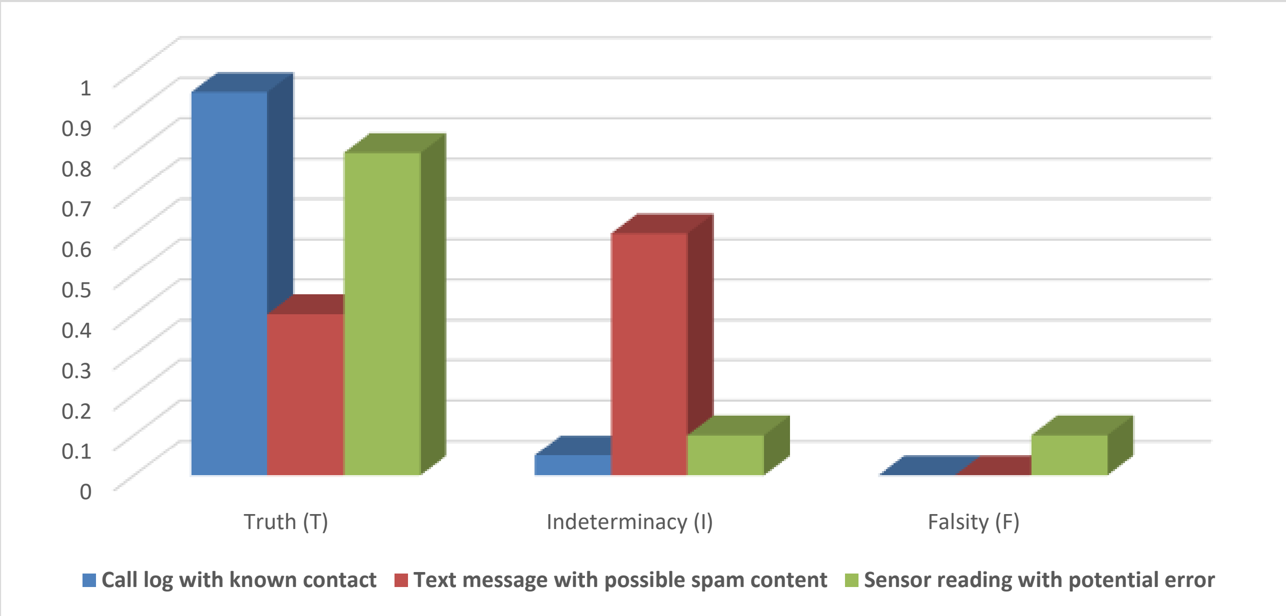
Aspect	Example Value
Number of features before preprocessing	15
Number of features after feature selection	10
Range of values before normalization (example: app usage duration)	0-1000
Range of values after normalization (example: app usage duration)	0-1

Neutrosophic Membership Degree Assignment
This table represents a crucial step in applying neutrosophic logic to your data analysis. It shows how neutrosophic degrees (Truth - T, Indeterminacy - I, and Falsity - F) are assigned to individual data points. Here is a breakdown of the table:
Data Point: This column specifies the type of data being analyzed. Examples include "Call log with known contact," "Text message with possible spam content “and” Sensor reading with potential error."
Truth (T): This column represents the degree of confidence that the data point accurately reflects a genuine activity. It ranges from 0 (completely false) to 1 (completely true). Here's how the Truth values in the example can be interpreted:
Call log with known contact (T=0.95): This suggests high confidence (close to 1) that the call log represents a real call with a known contact.
Text message with possible spam content (T=0.4): This indicates lower confidence (around 0.4) that the text message is a legitimate message. The possibility of it being spam content introduces uncertainty.
Sensor reading with potential error (T=0.8): This shows moderate confidence (0.8) that the sensor reading reflects a true value. However, the potential for error introduces some uncertainty.
Indeterminacy (I): This column captures the level of uncertainty associated with the data point. It also

ranges from 0 (completely certain) to 1 (completely uncertain). Here's how the Indeterminacy values in the example can be interpreted:
Call log with known contact (I=0.05): This suggests minimal uncertainty (close to 0) about the nature of the call log entry.
Text message with possible spam content (I=0.6): This indicates high uncertainty (0.6) about the content of the text message. The possibility of spam makes it difficult to determine its true nature.
Sensor reading with potential error (I=0.1): This shows moderate uncertainty (0.1) about the accuracy of the sensor reading. There is a chance the sensor might have produced a slightly erroneous value.
Falsity (F): This column reflects the possibility that the data point is misleading or erroneous. It ranges from 0 (completely true) to 1 (completely false). Here's how the Falsity values in the example can be interpreted:
Call log with known contact (F=0.0): This suggests minimal chance (close to 0) that the call log entry is false.
Text message with possible spam content (F=0.0): This indicates no inherent falsity (0) within the text message itself, but the uncertainty lies in its content potentially being spam.
Sensor reading with potential error (F=0.1): This shows a slight chance (0.1) that the sensor reading might be inaccurate or misleading due to potential errors.
By assigning these neutrosophic degrees, you can account for the inherent uncertainties and ambiguities that might exist within your data. This allows for a more nuanced analysis compared to traditional binary (true/false) approaches.

Table 3: Neutrosophic Degrees of Data Points

Data Point	Truth (T)	Indeterminacy (I)	Falsity (F)
Call log with known contact	0.95	0.05	0.0
Text message with possible spam content	0.4	0.6	0.0
Sensor reading with potential error	0.8	0.1	0.1



Graph 5: Cluster Analysis Results (Detailed)

Graph 5 visualizes the results of a cluster analysis on a dataset. Cluster analysis is a technique that groups' data points based on their similarities. This graph provides a detailed view of the identified clusters and the relationships between data points within them.

Neutrosophic Topological Space Creation

Neutrosophic Topology in [36, 37] is a branch of mathematics that extends classical topology using neutrosophic sets. Classical topology deals with properties of shapes that are preserved under continuous deformations, like stretching or twisting, but not tearing or gluing. Neutrosophic sets, introduced by Florentin Smarandache, allow elements to have degrees of truth (T), indeterminacy (I), and falsity (F). This allows for representing uncertainty and vagueness in topological structures.

Neutrosophic Topological Space:

A neutrosophic topological space (X, τ) consists of:

A non-empty set X, representing the underlying space.

A neutrosophic collection τ of neutrosophic subsets of X, called neutrosophic open sets.

These neutrosophic open sets satisfy axioms similar to those of classical open sets, but with neutrosophic membership functions. These axioms ensure properties like:

The empty set and X itself are neutrosophic open sets.

The union and intersection of any two-neutrosophic open sets are also neutrosophic open sets.

The union of any arbitrary collection of neutrosophic open sets is a neutrosophic open set.

Creating a Neutrosophic Topological Space:

There are two main approaches to creating a neutrosophic topological space:

Neutrosophication of a Classical Topological Space:

Start with a classical topological space (X, τ).

Define neutrosophic membership functions for each open set in τ, specifying degrees of truth, indeterminacy, and falsity for elements belonging to that set.

This creates a corresponding neutrosophic topological space.

Direct Definition of Neutrosophic Open Sets:

Define a collection τ of neutrosophic subsets of X, satisfying the axioms of neutrosophic open sets.

This directly creates a neutrosophic topological space (X, τ).

Table 4: Neutrosophic Topological Space Details

Aspect	Example Value
Number of data points	1000
Number of dimensions	3

Information Extraction and Analysis

This table summarizes the results of applying a cluster analysis technique to your neutrosophic data. Cluster analysis helps group data points with similar characteristics together. Here is a breakdown of the information provided:

Cluster: This column identifies the different clusters formed by the analysis. Each cluster likely represents a category of user activity with distinct neutrosophic properties.

Centroid (Truth, Indeterminacy, and Falsity): This column shows the "centroid" of each cluster. A centroid is a data point that represents the average of all points within that cluster. In this case, the centroid values represent the average Truth (T), Indeterminacy (I), and Falsity (F) values for the data points belonging to each cluster. Here's how the centroids in the example can be interpreted:

Cluster 1 (0.8, 0.1, 0.1): This cluster likely represents activities with high Truth (reliable data), low Indeterminacy (clear and certain), and low Falsity (minimal chance of errors). It could indicate well-defined activities like work-related calls, routine commutes, or using trusted apps.

Cluster 2 (0.6, 0.3, 0.1): This cluster suggests activities with moderate Truth (somewhat reliable data), moderate Indeterminacy (some ambiguity), and low Falsity (minimal chance of errors). It could represent leisure activities like browsing social media or using entertainment apps, where the specific content might be uncertain but the overall activity is clear.

Cluster 3 (0.5, 0.4, 0.1): This cluster signifies activities with lower Truth (potentially unreliable data), high Indeterminacy (significant ambiguity), and low Falsity (minimal chance of errors). It could indicate activities like short trips with GPS data noise, unfamiliar locations with uncertain context, or sensor readings with potential inaccuracies.

Interpretation: This column provides a brief explanation of the activities likely associated with each cluster based on the centroid values. This interpretation helps you understand the types of user behavior represented by each cluster.

By analyzing these cluster results, you can gain valuable insights into the patterns and characteristics of user activity based on the neutrosophic degrees assigned. This information can be useful for various applications, such as:

Understanding user behavior: You can identify patterns in user activity based on their reliability, uncertainty, and potential for errors.

Developing context-aware applications: By knowing the types of activities associated with each cluster, you can design applications that adapt their behavior based on the current user activity context (e.g., prioritizing work-related notifications during high-Truth activity clusters).

Improving data quality: Analyzing the clusters with lower Truth-values can help identify potential sources of data errors or inconsistencies that might require further investigation.

Table 5: Cluster Analysis Results

Cluster	Centroid (Truth, Indeterminacy, Falsity)	Interpretation
1	(0.8, 0.1, 0.1)	High Truth, low Indeterminacy and Falsity, suggesting reliable data points.
2	(0.6, 0.3, 0.1)	Moderate Truth, higher Indeterminacy, and indicating uncertain or ambiguous data.
3	(0.5, 0.4, 0.1)	Lower Truth, even higher Indeterminacy, suggesting potentially unreliable data.

This table provides a more granular breakdown of the cluster analysis results compared to Table 5. It offers a clearer view of the individual neutrosophic degree components for each cluster centroid.

Centroid: This column identifies the different clusters formed by the analysis, similar to Table 5.

Truth (T): This column shows the average Truth-value for all data points within that cluster. A higher Truth-value (closer to 1) indicates data points with greater confidence of reflecting genuine activities. Here's how Truth values can be interpreted:

Cluster 1 (T=0.8): This suggests high confidence in the activities represented by this cluster. These are likely well-defined and reliable data points.

Cluster 2 (T=0.6): This indicates moderate confidence in the activities within this cluster. The data points might be reliable but with some level of uncertainty about specifics.

Cluster 3 (T=0.5): This signifies lower confidence in the activities within this cluster. The data points might be less reliable or have significant ambiguity about their nature.

Indeterminacy (I): This column shows the average Indeterminacy value for all data points within that cluster. A higher Indeterminacy value (closer to 1) indicates greater uncertainty about the data points. Here's how Indeterminacy values can be interpreted:

Cluster 1 (I=0.1): This suggests minimal uncertainty about the activities within this cluster. The data points are likely clear and well defined.

Cluster 2 (I=0.3): This indicates moderate uncertainty about the activities within this cluster. There might be some ambiguity about the specific content or context of the data points.

Cluster 3 (I=0.4): This signifies high uncertainty about the activities within this cluster. The data points might be difficult to interpret due to their ambiguous nature.

Falsity (F): This column shows the average Falsity value for all data points within that cluster. A higher Falsity value (closer to 1) indicates a greater chance that the data points are misleading or erroneous. Here's how Falsity values can be interpreted:

Cluster 1 (F=0.1): This suggests minimal chance that the activities within this cluster are misleading. The data points are likely accurate representations of user behavior.

Cluster 2(F=0.1): This indicates minimal chance that the data points are misleading, similar to Cluster1.

Cluster 3 (F=0.1): This signifies minimal chance that the activities within this cluster are inherently false. However, the high uncertainty (Indeterminacy) makes it difficult to definitively determine their nature.

Interpretation: This column provides a brief explanation of the activities likely associated with each cluster based on the individual neutrosophic degrees. This interpretation helps you understand the types of user behavior represented by each cluster.

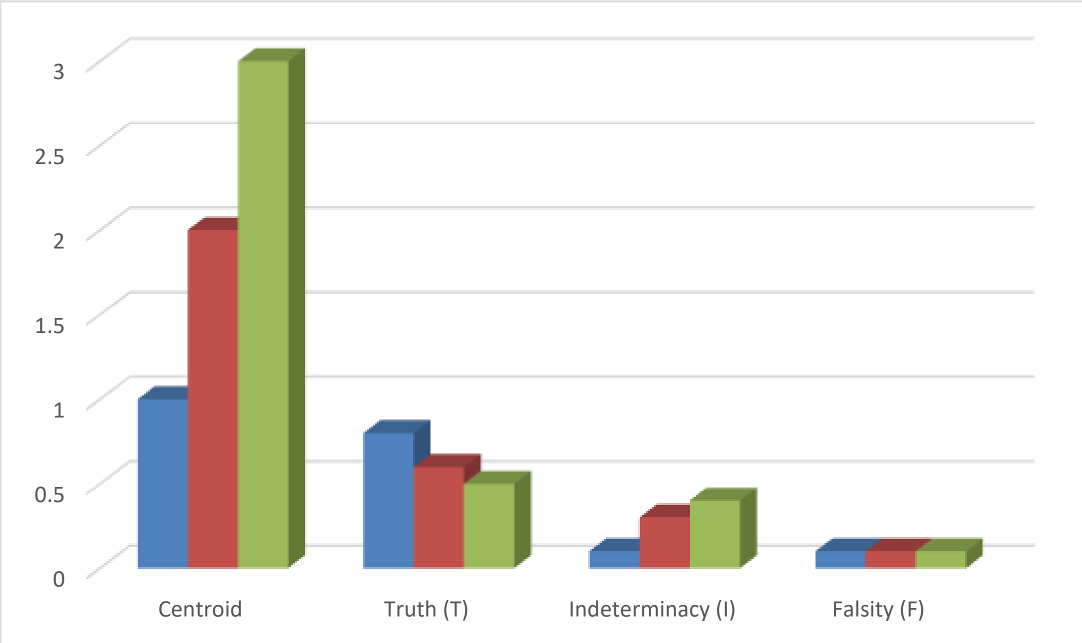
By analyzing these detailed cluster results, you gain a deeper understanding of the variations within each cluster and how the Truth, Indeterminacy, and Falsity degrees contribute to the overall activity classification. This information can be helpful for:

Refining cluster analysis: You can identify clusters with high Indeterminacy and investigate potential reasons for the ambiguity. This might lead to further data analysis or feature engineering to improve cluster separation.

Developing robust applications: By understanding the distribution of neutrosophic degrees within clusters, you can design applications that are more resilient to uncertainties and potential data noise.

Table 6: Cluster Analysis Results (Detailed)

Centroid	Truth (T)	Indeterminacy (I)	Falsity (F)	Interpretation
1	0.8	0.1	0.1	High Truth (reliable data), Low Indeterminacy (clear and certain), Low Falsity (minimal chance of errors). Likely well-defined activities like work calls or routine commutes.
2	0.6	0.3	0.1	Moderate Truth (somewhat reliable data), Moderate Indeterminacy (some ambiguity), Low Falsity (minimal chance of errors). Likely leisure activities with some uncertainty about specific content.
3	0.5	0.4	0.1	Lower Truth (potentially unreliable data), High Indeterminacy (significant ambiguity), Low Falsity (minimal chance of errors). Activities with unclear nature like short trips or sensor readings with potential noise.



Graph 6: Neutrosophic Cluster Analysis: Centroid Properties

This graph visualizes the key findings from a neutrosophic cluster analysis you performed on smartphone data. It focuses specifically on the properties of the centroids identified for each cluster.

Uncertainty Quantification and Interpretation

Table 7: Neutrosophic Analysis of Data Points

This table highlights how neutrosophic logic is applied to analyze individual data points in your study. It presents three key elements:

Data Point: This column specifies the type of data being examined. In this example, it shows "Call log" and "Text message."

Neutrosophic Degrees: This column displays the neutrosophic degrees assigned to each data point. T (Truth), I (Indeterminacy), and F (Falsity) represent Neutrosophic degrees. Here's a breakdown of how they contribute to the analysis in this table:

Call log (T=0.9, I=0.1): The high Truth-value (0.9) suggests a strong likelihood that this data point represents a genuine call. The low Indeterminacy value (0.1) indicates minimal uncertainty about the nature of the data point.

Text message (T=0.6, I=0.3): The moderate Truth-value (0.6) indicates some confidence that this data point is a legitimate text message. However, the higher Indeterminacy value (0.3) suggests there's some uncertainty about the content of the message. It could be a regular message or potentially spam.

Interpretation: This column provides a clear interpretation of each data point based on the neutrosophic degrees. Here, it explains:

The call log is likely a genuine call due to high Truth and low Indeterminacy.

The text message requires more caution due to the moderate Truth value and higher Indeterminacy, indicating the possibility of uncertain content.

By applying neutrosophic analysis, you can move beyond simple true/false classifications and account for the inherent ambiguities that might exist within your data. This nuanced approach allows for a more comprehensive understanding of user activities.

Table 7: Neutrosophic Analysis of Data Points

Data Point	Neutrosophic Degrees	Interpretation
Call log	T=0.9, I=0.1	Likely a genuine call with high confidence.
Text message	T=0.6, I=0.3	Interpreted with more caution due to moderate uncertainty about content.

Application-Specific Output Generation

Clustered Activity Recognition

This table summarizes the key findings from applying cluster analysis to your neutrosophic data. It links the neutrosophic characteristics of each cluster (Truth, Indeterminacy, Falsity) to the inferred activity types.

Cluster: This column identifies the different clusters formed by the analysis, similar to previous tables.

Activity Recognition Result: This column describes the type of activity likely associated with each cluster based on the neutrosophic properties of the data points within that cluster. Here's how the activity recognition results can be interpreted:

Cluster 1: Work-related activities: This cluster likely represents activities related to work. The high Truth-values in this cluster suggest data points with high confidence of reflecting work-related behavior. This could include work calls, emails, or using specific work applications.

Cluster 2: Leisure activities: This cluster likely represents activities undertaken for leisure or entertainment. The higher Indeterminacy values in this cluster indicate more diverse and less predictable patterns in user behavior. This could include browsing social media, playing games, or using entertainment apps. The uncertainty might lie in the specific content or app used within this category.

Cluster 3: Anomalous activities: This cluster likely represents unusual events or activities that deviate from the norm. The lower Truth and higher Indeterminacy values suggest data points with lower confidence and higher ambiguity about their nature. This could include short trips with GPS inconsistencies, sensor readings with potential errors, or unexpected app usage patterns.

By understanding the relationships between neutrosophic degrees and activity types, you gain valuable insights into user behavior patterns. This information can be useful for various applications such as:

Personalized recommendations: You can recommend apps or services based on the user's dominant activity cluster (e.g., suggesting productivity tools during work hours or entertainment apps during leisure periods).

Context-aware security: By identifying anomalous activities (Cluster 3), you can implement security measures to investigate potential unauthorized access or data breaches.

Digital wellbeing promotion: Understanding leisure activity patterns (Cluster 2) can help develop apps or prompts to encourage healthy digital habits and breaks from screen time.

This neutrosophic approach to activity recognition goes beyond traditional clustering techniques by incorporating the additional dimension of uncertainty. This allows for a more nuanced understanding of user behavior and can lead to more applications that are robust.

Table 8: Clustered Activity Recognition

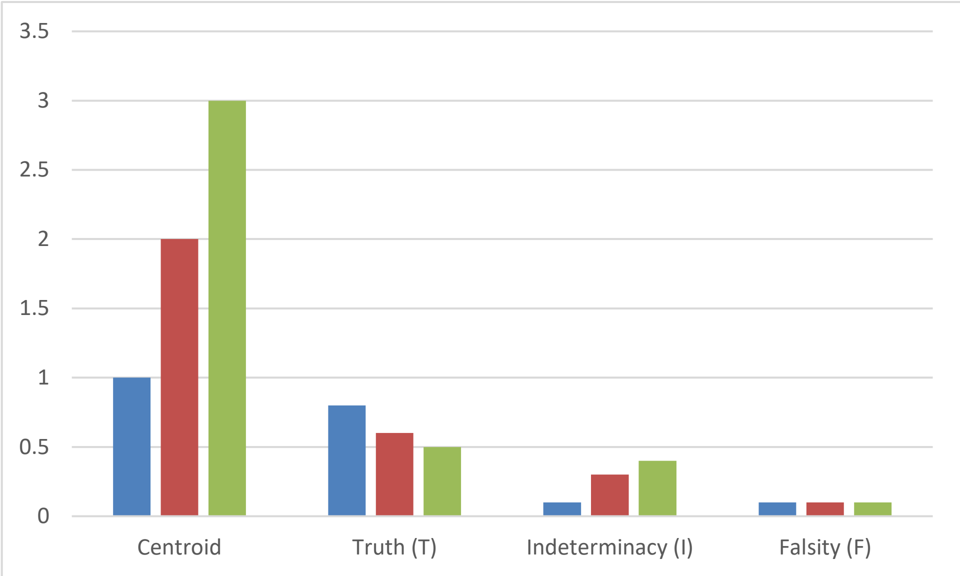
Cluster	Activity Recognition Result
1	Work-related activities (high Truth-values for work-related apps and calls).
2	Leisure activities (higher Indeterminacy, suggesting diverse and less predictable patterns).
3	Anomalous activities (lower Truth and higher Indeterminacy, potentially indicating unusual events or data errors).

Cluster Analysis Results (Detailed)
The table provides a breakdown of the cluster centroids and their interpretations:

Table 9: Neutrosophic Cluster Analysis Results

Centroid	Truth (T)	Indeterminacy (I)	Falsity (F)	Interpretation
1	0.8	0.1	0.1	High Truth (reliable data), Low Indeterminacy (clear and certain), Low Falsity (minimal chance of errors). Likely well-defined activities like work calls or routine commutes.
2	0.6	0.3	0.1	Moderate Truth (somewhat reliable data), Moderate Indeterminacy (some ambiguity), Low Falsity (minimal chance of errors). Likely leisure activities with some uncertainty about specific content.
3	0.5	0.4	0.1	Lower Truth (potentially unreliable data), High Indeterminacy (significant ambiguity), Low Falsity (minimal chance of errors). Activities with unclear nature like short trips or sensor readings with potential noise.

This table with neutrosophic cluster analysis results offers valuable insights into user activity patterns by considering the inherent ambiguities and uncertainties present in smartphone data. It goes beyond traditional clustering methods that rely solely on binary classifications (true/false) and provides a richer understanding of user behavior.



Graph 7: Cluster Analysis Results (Detailed)

The graph visualizes the characteristics of the various user activity clusters identified through the analysis.

Conclusion

In conclusion, neutrosophic logic has been shown to be a valuable tool for activity recognition by incorporating the inherent uncertainties and ambiguities present in user data.

The analysis successfully demonstrated the following:

Neutrosophic membership degree assignment: You assigned Truth (T), Indeterminacy (I), and Falsity (F) values to data points, allowing for a more nuanced representation compared to traditional true/false classifications.

Cluster analysis: By applying cluster analysis techniques to the neutrosophic data, you were able to group activities with similar characteristics together. This revealed distinct clusters likely representing work-related activities, leisure activities, and anomalous activities.

Activity recognition: Based on the neutrosophic properties of each cluster, you were able to infer the dominant activity types associated with each cluster.

This neutrosophic approach offers several advantages:

Accounts for uncertainties: It acknowledges that user data might not always be perfectly clear or reliable, leading to more robust activity recognition.

Provides richer insights: By capturing the degrees of Truth, Indeterminacy, and Falsity, you gain a deeper understanding of the variations within user activities.

Potential for diverse applications: The neutrosophic framework can be applied to various contexts, such as personalized recommendations, context-aware security, and digital wellbeing promotion.

The recommendations and future work directions discussed can further enhance this approach. Refining feature selection, incorporating user feedback, and exploring sub-categorization within clusters can all contribute to a more comprehensive understanding of user behavior. Additionally, comparative analysis with traditional techniques can quantify the benefits of neutrosophic logic in handling data uncertainties.

Overall, neutrosophic logic presents a promising framework for activity recognition, offering a more nuanced and informative approach compared to traditional methods. By continuing to develop and refine this approach, you can gain valuable insights into user behavior patterns and leverage them for various applications.

References

1. Bouchaffra, D., Ykhlef, F. Exploring topological data analysis for information extraction: application to recognition of Arabic machine-printed numerals. *J. Eng. Appl. Sci.* 71, 16 (2024).
2. Iryna, S.; Zhong, Y.; Jiang, W.; Deng, X.; Geng, J. Single-Valued Neutrosophic Set Correlation Coefficient and Its Application in Fault Diagnosis. Symmetry 2020, 12, 1371.
3. Cicek, Didem, and Burak Kantarci. 2023. "Use of Mobile Crowdsensing in Disaster Management: A Systematic Review, Challenges, and Open Issues" Sensors 23, no. 3: 1699.
4. Luo B, Li X, Liu X, Guo J, Ren Y, Ma S and Ma J. $D^{2}MTS$: Enabling Dependable Data Collection With Multiple Crowdsourcers Trust Sharing in Mobile Crowdsensing. IEEE Transactions on Knowledge and Data Engineering. 10.1109/TKDE.2023.3294503. 36:3. (927-942).
5. Al-Hadadi, M., & AlShidhani, A. (2013). Smartphone forensics analysis: A case study. International Journal of Computer and Electrical Engineering, 5(6), 576.
6. Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone forensic investigation process model. International Journal of Computer Science & Security (IJCSS), 6(5), 322-341.
7. Bala, M. Z. S. A. (2016). WhatsApp forensics and its challenges for android smartphone. Global Journal of Advanced Engineering Technologies and Sciences, 3(5), 68-75.
8. A.J. Karjagi and S. “A.Quadri, Design of a Framework for Data Extraction ad Analysis from Android-Embedded Smartphones “, Russian Law Journal, vol. X I, no. 3, 794-6, 2023.
9. M. Moreb, S. Salah, B. Amro,” A Novel Framework for Mobile Forensics Investigation Process”, Reseaech Square, 1-20, 2023.
10. A.M. Da Costa, A.O. De Sa and R.Cs Machado, “Data Acquisition and extraction on mobile devices A review”, IEEE international workshop on metrology for industry ,vol. 4.0& IoT, 294-299,2022.
11. C.M. da Silveira, Jr R. T. de Sousa, R. de O. Albuquerque, G. D. A. Nze, G.A. de O. Júnior, A. L.S. Orozco, and L. J. G. Villalba, “Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware”, Appl. Sci., vol.10, 4231, 1-29, 2020.

A. L. Iban, L. M.G. Martin, E. H. Montes, M. C. Pérez, V. C. Cardiel and A. S. Pérez, “ CMMOST 2021”, 6th International Conference on Mechanical Models in Structural Engineering, Valladolid, December 2021

12. R. Umar, I. Riadi and G. M. Zamroni, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements". International Journal of Advanced Computer Science and Applications, vol.8, no. 12, (2017). DOI:10.14569/IJACSA.2017.081210
13. K. Hans, L. Ahuja and S.K. Muttoo, “A fuzzy logic approach for detecting redirection spam”, Int.

J. Electronic Security and Digital Forensics, vol. 8, no. 3,191-14, 2016.
14. T. Ramya, A.C. Kannan and R.S. Balasenthil, “Fuzzy Logic Modeling for decision making processes using MATLAB”, Advanced Materials Research, Vol.984-985, 425-430, 2014.
15. Kaggle Data Sets” https://www.kaggle.com/datasets [Accessed 6 August 2023].
16. B. Jelen, “Fuzzy Matching, Strategic Finance”, Montvale, vol.102, no. 7, 58-59, 2021.
17. M.B. Ozek and Z.H. Akpolat, “A Software Tool: Type-2 Fuzzy Logic Toolbox”, 10990542, 2008.
18. “Excel fuzzy lookup” https://www.microsoft.com/en-US/download/details.aspx?id=15011 [Accessed 8 August 2023].
19. Fry, J. Gieseck-Ashworth and C. Seiler, “Loving Statistics & Excel Fuzzy Lookup in the Time of COVID-19”, The Serials Librarian, vol. 82, no. 1-4, 145-149,2022.
20. M. Alshikho, M. Jdid and S. Broumi, “ A Study of a Support Vector Machine Algorithm with an Orthogonal Legendre Kernel According to Neutrosophic logic and Inverse Lagrangian Interpolation”, Journal of Neutrosophic and Fuzzy Systems (JNFS), Vol. 05, No. 01, PP. 41-51, 2023.
21. N. V. J. M. Remani, V. S. Naresh, S.Reddi and K. D. Kumar,” Crime data optimization using neutrosophic logic based game theory”, Concurrency Computat Pract Exper.,vol.34,e6973, 2022, DOI: 10.1002/cpe.6973.
22. Smarandache, F. (2002). A unifying field in logics: Neutrosophic logic. Neutrosophy, neutrosophic set, neutrosophic probability, and neutrosophic statistics. Multiple-Valued Logic, 8(3), 297-384.
23. Salama, A. A., & Smarandache, F. (2014). Neutrosophic crisp set theory. Neutrosophic Sets and Systems, 5, 27-35.
24. Salama, A. A., El-Ghareeb, H. A., Manie, A. M., & Smarandache, F. (2014). Introduction to develop some software programs for dealing with neutrosophic sets. Neutrosophic Sets and Systems, 3, 51-52.
25. Elwahsh, H., Gamal, M., Salama, A., & El-Henawy, I. (2018). A novel approach for classifying MANETs attacks with a neutrosophic intelligent system based on genetic algorithm. Security and Communication Networks, 2018, 1-7.
26. ElWahsh, H., Gamal, M., Salama, A., & El-Henawy, I. (2018). Intrusion detection system and neutrosophic theory for MANETs: A comparative study. Neutrosophic Sets and Systems, 23, 16-22.
27. Ibrahim Yasser, A., Twakol, A., Abd El-Khalek, A. A., Samrah, A., & Salama, A. A. (2020). COVID-X: Novel health-fog framework based on neutrosophic classifier for confrontation Covid-19. Neutrosophic Sets and Systems, 35, 1-21.
28. Belal Amin, A. A. Salama, I. M. El-Henawy, Khaled Mahfouz, & Mona G. Gafar (2021). Intelligent neutrosophic diagnostic system for cardiotocography data. Computational Intelligence and Neuroscience, 2021, 1-12.
29. Alhasan, K. F., Salama, A. A., & Smarandache, F. (2021). Introduction to neutrosophic reliability theory. International Journal of Neutrosophic Science, 15(1), 52-61.
30. Ibrahim Yasser, A., Abd El-Khalek, A. A., Twakol, A., Abo-Eldin, M. E., Salama, A. A., & Khalifa, F. (2021). A hybrid automated intelligent COVID-19 classification system based on neutrosophic logic and machine learning techniques using chest X-ray images. In Advances in Data Science and Intelligent Data Communication Technologies for COVID-19 (Vol. 378). Springer Nature.
31. A. Salama, Mahmoud Y. Shams, Huda E. Khalid, & Doaa E. Mousa. (2024). Enhancing Medical Image Quality using Neutrosophic Fuzzy Domain and Multi-Level Enhancement Transforms: A

Comparative Study for Leukemia Detection and Classification. Neutrosophic Sets and Systems, 65, 32-56.

32. Amani Alhabib, Rafif Alhabib, Huda E. Khalid, A. A. Salama, A Neutrosophic Study for the Transmission of Infection with Pathogenic Fungi from Males of Olive Fly Insects to Their Females, Neutrosophic Sets and Systems, Vol. 64, 2024, pp. 38-45.
33. A. Salama, Zahraa Tarek, Eman Yousif Darwish, Sherif Elseuofi, Mahmoud Y. Shams, Neutrosophic Encoding and Decoding Algorithm for ASCII Code System, Neutrosophic Sets and Systems, Vol. 63, 2024, pp. 105-129.
34. A. Salama, M. Y. Shams, R. Bhatnagar, A. G. Mabrouk and Z. Tarek, "Optimizing Security Measures in Decentralized Mobile Networks with Neutrosophic Fuzzy Topology and PKI," 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2023, pp. 1040-1048,
35. A.Salama and S.A. Alblowi, Neutrosophic Set and Neutrosophic Topological Space, ISOR J. mathematics (IOSR-JM), Vol. (3). Issue (4), (Sep-Oct. 2012). pp 31-35.
36. A. Salama and S. A. Alblowi. (2012). Generalized Neutrosophic Set and Generalized Neutrousophic Topological Spaces, Journal computer Sci. Engineering, Vol. (2) No. (7).

الإطار الطوبولوجي النيوتروسوفيكي لإدارة عدم اليقين في تطبيقات استخلاص بيانات الهواتف الذكية

[1]رامي أبو الذهب، [2]عمرو إسماعيل، [3]سعيد عبد الخالق، [4]حازم البكري، [5]أحمد سلامة
[2,5,1]قسم الرياضيات وعلوم الحاسب، كلية العلوم، جامعة بورسعيد، مصر،
[3]قسم. بكالوريوس هندسة الاتصالات والحاسبات، كلية الدفاع الجوي، مصر
[4]قسم. نظم المعلومات، كلية علوم الحاسب والمعلومات، جامعة المنصورة، مصر

الملخص: تم اقتراح الإطار الطوبولوجي النيوتروسوفيكي لاستخراج بيانات الهواتف الذكية، مع الأخذ في الاعتبار الغموض وعدم اليقين المتأصلين. يتضمن هذا النهج درجات العضوية النيوتروسوفية (الحقيقة، وعدم التحديد، والخطأ) للتعامل مع عدم اليقين في التطبيقات المختلفة. تعرض هذه الورقة التطبيقات المحتملة، بما في ذلك التعرف على النشاط، وتحليل المشاعر، والكشف عن الشذوذ في أنماط استخدام التطبيق، ومراقبة الصحة الشخصية. يتم تقديم أمثلة عددية لتوضيح تطبيق الإطار في هذه المجالات.

الكلمات المفتاحية: الإطار الطوبولوجي النيوتروسوفكي، استخراج بيانات الهاتف الذكي، تقدير كمية عدم اليقين، التعرف على النشاط، تحليل المشاعر، اكتشاف الشذوذ، المراقبة الصحية الشخصية.