The Role of Neutrosophic Logic in Enhancing Trust and Reliability in Internet of Things Architectures

Remya P. George[1], Nazia Ahmad[1], Rubina Liyakat Khan[1], Sajithunisa Hussain[1], Samandarboy Sulaymanov[2], Ambuj Kumar Agarwal[3,*]

[1]Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University, Saudi Arabia
[2]Tashkent State University of Economics, Tashkent, Uzbekistan
[3]Department of Computer Science and Engineering, Sharda School of Engineering and Technology, Sharda University, Greater Noida, India

Emails: rpgeorge@iau.edu.sa; nahmad@iau.edu.sa; rlkhan@iau.edu.sa; sajithunisa@iau.edu.sa; s.sulaymanov@tsue.uz; ambuj4u@gmail.com

Abstract

A vast amount of Internet of Things (IoT) devices deployment has created huge issues about trust management and reliability guarantees in heterogeneous, dynamic and often uncertain ecosystems. Available probabilistic or fuzzy-logic-based models do not hold water to deal with indeterminacy and contending data in distributed IoT networks. The current paper proposes a brand new framework to model trust and reliability in IoT systems by implementing Neutrosophic Logic to build quantification and strengthen trust and reliability in IoT systems. Incorporating the semantic understanding of data and node behavior in uncertainty using three dissimilar elements to represent trust: truth, indeterminacy and falsity, the model commands a wider range of semantics in the relationship of data and nodes during the phase of uncertainty. A mathematical solution is established to measure trust scores and reliability indexes based on Neutrosophic membership functions. Further, a new dynamic trust assessment and anomaly detection algorithm is presented based on a multi-layered decision-making process. This simulation and case- study definition shows the effectiveness of the proposed framework in having less false positives, better reliability estimation, and the solid optimization of decision support in a very uncertain environment of IoT. The work therefore further develops the process of Neutrosophic systems integration with IoT and its setting up of basis of more intelligent, context-aware and robust trust management systems.

Keywords: Neutrosophic Logic; internet of things (IoT); Trust management; Reliability modeling; Indeterminacy; Uncertainty quantification; Mathematical modeling; Decision support systems

1 Introduction

Internet of Things (IoT) is a disruptive technological framework in which trillions of interactions between devices, sensors, and actuators create and share data without any intervention. The need to ensure secure communication of trustful data and reliable functioning of the system also grows along with the complexity and the scale of the IoT system. Available trust and reliability are thus no longer optional (but mandatory) properties, as required in enabling mission-critical application domains in healthcare monitoring, autonomous transport, smart grids, and industrial automation.

Otherwise, in such distributed architectures heterogeneous IoT devices tend to be used under resource limitations, to communicate by problematic wireless channels, and have to face malicious attacks or failures. Such

conditions create significant difficulty in the development and preservation of relationships of trust between devices, particularly in instances whereby conventional models use static or binary assumptions on the behaviour of nodes. Furthermore, dynamically contextual model of IoT data flow due to its nature transverses data and requires a more freeform and fluid framework to measure trustworthiness and dependability.[1]

Trust management has extensively used classical methodologies such as probabilistic models, Bayesian inference and fuzzy logic. They are nevertheless limited when it comes to their ability to deal with vacuity as well as indeterminacy at the same time. An example of such is the fuzzy logic, which makes some allowance of partial truth but fails to explicitly represent circumstances where the information is conflicting or incomplete.[1] Probabilistic models rely strongly on prior knowledge or assumptions on the distribution, which are hard to be checked when using real-time IoT systems.

In order to overcome these shortfalls, Neutrosophic Logic has come as an effective generalisation of classical and fuzzy logics systems. Neutrosophic Logic, proposed by Florentin Smarandache defines three independent elements, namely: truth (T), indecisiveness (I), falsity (F) that has values in either the real non-standard or standard interval: $[0^-, 1^+]$. This triple representation gives the logic the ability to solve the lack of clarity, the ambiguity and the conflict in the IoT data and device behaviour.[1]

The current research paper focuses on how to use Neutrosophic Logic to fit into a trust-reliability system that can be used to improve computational inference within the Internet-of-Things (IoT) networks. They state that the methodological possibilities presented through the Neutrosophic Logic, especially the ability of the brand to accommodate determinacy, uncertainty, partiality, and conflict all at once, make it a suitable tool to process data routes that IoT-centric dynamically changing networks may present.

The so-called trust-reliability model, that is proposed, comes up with the mathematical formulism where each node or transaction would each have inscribed in it the Neutrosophic membership function whose temporal evolution describes their behavior. This is followed by the instantaneous assessment of these membership functions followed, thereafter, by an iteration process that in a continuous and adaptive way, modifies the trust and reliability scores. One of the bright essentials of the model lies in the fact that it includes the usage of temporal feedback mechanisms and paradigms of indeterminate reasoning. By this regard, the framework can accommodate both centralised and distributed computing infrastructure, an attribute that is consistent with the heterogeneous deployment paradigm that is characteristic of fog and edge computing levels.

An outline of an additional decision-making algorithm is introduced, and it utilizes Neutrosophic inference processes in order to terminate dynamic identification of observed behaviours and detect anomalies. The algorithm has the ability to identify deviations in behavioral profiles and identify malicious nodes and reconcile the conflicting observations by the deployment of the Neutrosophic entropy and similarity measures rather than employing a set of dichotomous classification schemes. Such an inferential approach provides more adequate and strong basis of trust-based decision-making in practical IoT environments.

Experimetal validations were done using simulations using synthetic and benchmark IoT data. The experiment was evaluated with regards to the accuracy of trust, false-positive rate, the resilience of the system to noise and attack and efficiency of the system. Appropriate comparative evaluations with counterpart fuzzy-logic and probabilistic approaches indicated significant enhancements in reliability and robustness in situations of uncertainty thus justifying the acceptability of the Neutrosophic-trust-reliability schema proposed.

This paper contributes to the growing literature on intelligent trust frameworks by presenting the first comprehensive Neutrosophic-based trust-reliability architecture for IoT systems. It also provides a flexible mathematical toolset for future extensions involving multi-agent collaboration, data fusion, and self-adaptive systems in decentralized environments.

The remainder of this paper is organized as follows: Section 2 reviews related literature and foundational concepts in Neutrosophic Logic and trust modeling. Section 3 outlines the system architecture and defines the problem. Section 4 presents the proposed Neutrosophic mathematical model, while Section 5 describes the implementation framework and algorithms. Section 6 discusses the simulation setup. Section 7 results and performance evaluation. Finally, Section 8 concludes the paper and outlines future directions.

2 Background and Related Work

Neutrosophic Logic (NL), proposed as a generalization of fuzzy and intuitionistic logic, has gained momentum for handling indeterminacy and uncertainty in real-world systems. Unlike traditional binary or probabilistic systems, NL introduces a triad of membership degrees—truth (T), indeterminacy (I), and falsity (F)—which can model incomplete, inconsistent, or ambiguous data with greater flexibility.[12]

Recent advances have seen NL applied in diverse domains, from sentiment analysis[4] and education systems,[5] to health diagnostics[7,13,14] and agriculture.[10] In particular,[7] demonstrated the effectiveness of hybrid CNN-LSTM models augmented with Neutrosophic sets for dorsalgia prediction, reflecting NL's potential in uncertainty-rich biomedical datasets. Similarly,[?] explored the role of social media and AI tools like ChatGPT in educational evaluation, utilizing neutrosophic sets to interpret subjective student feedback.

In the IoT context, trust estimation frameworks have evolved to deal with sensor unreliability, spoofing, and anomalous behavior. Conventional models such as Fuzzy Logic Trust (FLT) and Bayesian Trust Estimation (BTE) offer partial handling of uncertainty. However, as shown in,[4] NL provides a more nuanced treatment, capturing indeterminacy due to transient or unexplained sensor states. Furthermore,[6] proposed a Li-Fi and IoT-based livestock monitoring system, emphasizing the need for reliable and trustable communication in animal care environments, where NL integration could enhance robustness.

The foundational expansion of NL into sets like Neutrosophic Over-/Under-/Off-Sets and Plithogenic sets, as introduced in,[9] further extends its application versatility.[11] applied these logics to crime prediction and spatial clustering, revealing that reliability analysis benefits significantly from handling partial truths and multi-faceted evidence.

The integration of NL into real-time cyber-physical systems was examined in works like,[8] which developed an IoT-based gas leakage detection system leveraging trust metrics for safe communication. This aligns with NL's emphasis on confidence-driven decision-making under uncertain event propagation.

From a regional application perspective, several studies have applied neutrosophic theory to economic and developmental data from Uzbekistan. For instance,[15] and[16] utilized NL to explore innovation dynamics and the influence of fiscal policy on poverty, respectively. These cases exemplify the model's generalizability beyond technical systems, fostering policy insight under ambiguity.

In the realm of learning analytics,[17] provided a critical dataset (OULAD) that, although not inherently neutrosophic, has been adapted in subsequent work for uncertainty-aware learner modeling—setting a precedent for applying NL in educational technology.

In summary, while FLT and BTE offer foundational approaches to trust evaluation in IoT networks, the emerging body of work points toward NL's superior ability to encode uncertainty and support real-time, confidence-weighted decision systems. The current research builds upon these insights by developing a Neutrosophic Logic-based trust-reliability model that integrates dynamic entropy, real-time behavior classification, and scalable fog deployment.

3 System Architecture and Problem Definition

3.1 System Architecture Overview

The proposed IoT trust-reliability framework consists of a layered architecture with heterogeneous devices such as sensors, actuators, and edge nodes communicating over wireless networks and transmitting data to cloud or fog-based analytics engines. Each node contributes to the overall system function (e.g., monitoring, control, alert generation), and its trustworthiness and reliability must be dynamically evaluated based on the behavior and contextual data it produces.

Figure 1 illustrates the overall architecture. The architecture consists of four layers:

- **Perception Layer**: Comprises diverse sensors S_i deployed for environmental sensing, health monitoring, industrial automation, etc.
- **Network Layer**: Handles data transmission via wireless (Wi-Fi, ZigBee, 5G) or wired protocols.
- **Edge/Fog Layer**: Performs local computation and preliminary trust evaluation.
- **Cloud Layer**: Hosts the centralized trust-reliability model, aggregation logic, and decision-making system.

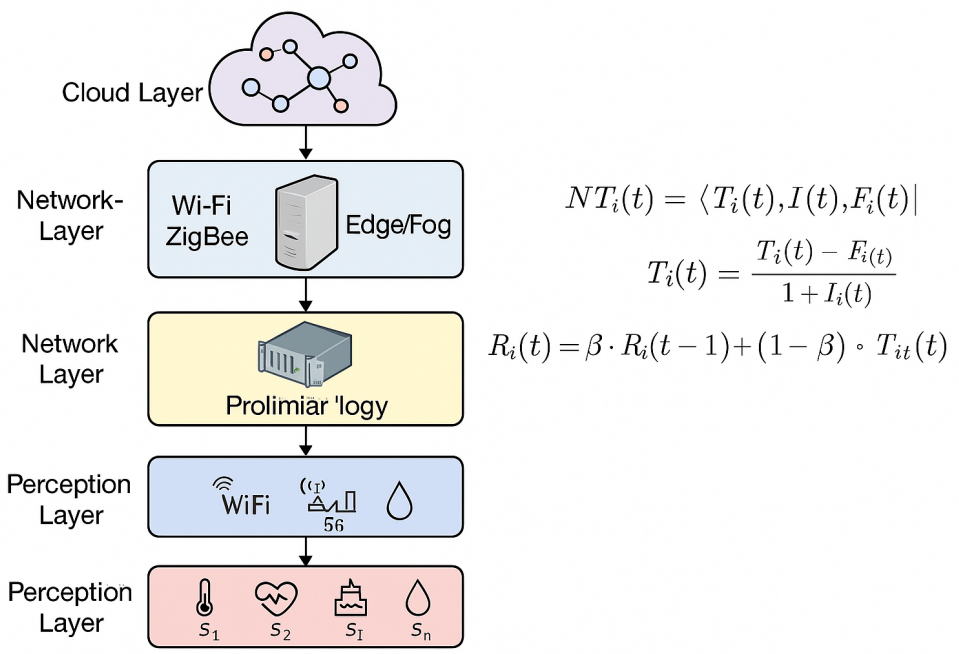

Figure 1: Neutrosophic-based Trust and Reliability Framework in IoT Architecture

3.2 Problem Statement

Let $S = \{S_1, S_2, \ldots, S_n\}$ be the set of n sensors in the IoT network. Each sensor S_i periodically transmits data $d_i(t)$ at time t to a central or edge processing unit. Our objective is to compute a dynamic trust score $\mathcal{T}_i(t)$ and a reliability score $\mathcal{R}_i(t)$ for each sensor using Neutrosophic Logic principles, which account for:

- The proportion of truthful behavior: $T_i(t)$
- The degree of indeterminacy: $I_i(t)$
- The proportion of false behavior: $F_i(t)$

The goal is to derive an accurate, context-aware, and adaptable mathematical model that evaluates $\mathcal{T}_i(t)$ and $\mathcal{R}_i(t)$ under uncertainty, conflicting evidence, and dynamic behavior.

3.3 Mathematical Model for Neutrosophic Trust Evaluation

Each sensor S_i at time t is represented by a neutrosophic trust tuple:

$$\mathcal{NT}_i(t) = \langle T_i(t), I_i(t), F_i(t) \rangle \tag{1}$$

Where:

- $T_i(t)$: The proportion of correct, valid, or expected behavior from S_i
- $F_i(t)$: The proportion of observed anomalies, incorrect, or malicious behavior
- $I_i(t)$: The level of indeterminacy or uncertainty in evaluating S_i at time t

Let w_1, w_2, w_3 be the weights for T, I, and F, respectively, such that $w_1 + w_2 + w_3 = 1$. The neutrosophic trust score is computed using:

$$\mathcal{T}_i(t) = \frac{T_i(t) - F_i(t)}{1 + I_i(t)} \tag{2}$$

This equation ensures that higher indeterminacy reduces trust, while a high truth-falsity gap increases it. The denominator stabilizes the result under uncertainty.

3.4 Modeling Sensor Behavior Metrics

Each sensor's behavior is tracked over a sliding time window W of size k. For each window, we compute:

$$T_i(t) = \frac{\text{Number of correct observations}}{k} \tag{3}$$

$$F_i(t) = \frac{\text{Number of incorrect observations}}{k} \tag{4}$$

$$I_i(t) = 1 - (T_i(t) + F_i(t)) \quad \text{(if not all samples classified)} \tag{5}$$

Let $\delta_j \in \{0, 1\}$ represent binary classification of the j^{th} observation as correct (1) or false (0). Then:

$$T_i(t) = \frac{1}{k}\sum_{j=1}^{k} \delta_j, \quad F_i(t) = \frac{1}{k}\sum_{j=1}^{k}(1 - \delta_j) \tag{6}$$

If some observations are missing or undecidable, $I_i(t)$ adjusts to reflect that uncertainty.

3.5 Reliability Index Based on Temporal Consistency

In addition to trust, we define a reliability score $\mathcal{R}_i(t)$ that reflects the long-term consistency and stability of the sensor:

$$\mathcal{R}_i(t) = \beta \cdot \mathcal{R}_i(t-1) + (1 - \beta) \cdot \mathcal{T}_i(t) \tag{7}$$

Where $\beta \in [0, 1]$ is a smoothing factor giving weight to past reliability history. Higher β means stronger inertia or memory in reliability evaluation.

3.6 Trust Thresholding and Classification

We define a threshold θ such that:

$$\text{If } \mathcal{T}_i(t) < \theta \Rightarrow \text{Sensor } S_i \text{ is untrustworthy}$$

This helps filter out faulty, compromised, or uncooperative nodes from the IoT network.

3.7 Formal Problem Definition

Given an IoT system with n sensors and their continuous data streams over time, the problem is to compute for each S_i:

- $\mathcal{NT}_i(t) = \langle T_i(t), I_i(t), F_i(t) \rangle$
- $\mathcal{T}_i(t)$ using Equation 11
- $\mathcal{R}_i(t)$ using Equation 15

The ability to ensure that trust and reliability scores improve in the face of uncertainty, dynamically sequential, and computationally efficient is an important requirement to the real world.

4 Neutrosophic Mathematical Trust-Reliability Model

In this part, we develop an applied mathematical model to trust and reliability modeling in Internet-of-Things (IoT) system by using Neutrosophic Logic (NL) formalism. In contrast to binary-/fuzzy-based systems, NL incorporates all truth, indeterminacy, and falsity, so, NL allows rigorous reasoning in a setting of uncertainty, inconsistency of sensors, and adversarial behavior typical of heterogeneous IoT networks.

4.1 Neutrosophic Representation of IoT Node Behavior

The index S_i can specify a sensor or a node in the Internet-of-Things and the $\mathcal{D}_i = \{d_i(t_1), d_i(t_2), \ldots, d_i(t_k)\}$ denotes the series of observations that is observed on S_i over a set window of time of a length k. Each and every $d_i(t_j)$ is exposed to a domain-utility validation processes or the existence of ground truth data. Based on this, we place a binary indicator $\delta_i(t_j)$ to each $d_i(t_j)$ labeling it either correct or wrong.

$$\delta_i(t_j) = \begin{cases} 1, & \text{if } d_i(t_j) \text{ is valid or expected} \\ 0, & \text{if } d_i(t_j) \text{ is invalid, inconsistent, or missing} \end{cases}$$

Through these labels, the three Neutrosophic parts of the observation tied into d(t) are as below:

$$T_i(t) = \frac{1}{k} \sum_{j=1}^{k} \delta_i(t_j) \tag{8}$$

$$F_i(t) = \frac{1}{k} \sum_{j=1}^{k} (1 - \delta_i(t_j)) \tag{9}$$

$$I_i(t) = 1 - [T_i(t) + F_i(t)] \tag{10}$$

By introducing a latent indicator variable $I_i(t)$ it is possible to include missing or unclassified observations in a stochastic differential equation model. This way, the state-space model obtained continues to be valid and a representation of the empirical reality even through heterogeneous and noisy data.

4.2 Neutrosophic Trust Score Function

We define the trust score of node S_i at time t using a normalized difference model as follows:

$$\mathcal{T}_i(t) = \frac{T_i(t) - F_i(t)}{1 + I_i(t) + \epsilon} \tag{11}$$

Here, $\epsilon > 0$ is a small constant to avoid division by zero. The trust score $\mathcal{T}_i(t)$ satisfies the following constraints:

- $\mathcal{T}_i(t) \in [-1, +1]$ - If $T_i = 1$ and $F_i = 0$, then $\mathcal{T}_i \approx 1$ (perfect trust) - If $T_i = 0$ and $F_i = 1$, then $\mathcal{T}_i \approx -1$ (malicious behavior) - When $I_i(t) \to 1$, trust score magnitude diminishes, reflecting uncertainty

This model captures both the direction (trust vs. distrust) and confidence (low indeterminacy) of evaluation.

4.3 Weighted Trust Score Model

To incorporate system-specific priorities, we define a weighted scalar trust score:

$$NS_i(t) = w_T \cdot T_i(t) + w_I \cdot (1 - I_i(t)) - w_F \cdot F_i(t) \tag{12}$$

Subject to $w_T, w_I, w_F \in [0, 1]$ and $w_T + w_I + w_F = 1$. This allows system designers to emphasize certain aspects:

- $w_T \gg w_F$ for trust-optimistic networks - $w_F \gg w_T$ for conservative, security-critical applications - $w_I \gg 0$ for uncertainty-aware decisions

4.4 Temporal Trust Aggregation and Stability

IoT systems are dynamic, hence a single observation cannot be used to permanently define trust. We propose temporal aggregation using exponential moving averages:

$$\mathcal{T}_i^{\text{agg}}(t) = \alpha \cdot \mathcal{T}_i^{\text{agg}}(t-1) + (1 - \alpha) \cdot \mathcal{T}_i(t) \tag{13}$$

Where $\alpha \in [0, 1]$ controls temporal memory:

- $\alpha \to 1$: Emphasizes historical consistency (slow updates) - $\alpha \to 0$: Quickly adapts to new behavior

This trust score is more robust in fluctuating environments.

4.5 Reliability Modeling Based on Temporal Volatility

Reliability is interpreted as the temporal regularity of trust behavior. A node that frequently switches between trust and distrust is considered unreliable. We define the volatility of a node as:

$$\Delta\mathcal{T}_i(t) = |\mathcal{T}_i(t) - \mathcal{T}_i(t-1)| \tag{14}$$

And compute reliability using:

$$\mathcal{R}_i(t) = \beta \cdot \mathcal{R}_i(t-1) + (1 - \beta) \cdot (1 - \Delta\mathcal{T}_i(t)) \tag{15}$$

Where β is a temporal decay factor. The term $1 - \Delta\mathcal{T}_i(t)$ penalizes large swings in trust. If trust is stable, the node gains reliability over time.

4.6 Entropy-Based Uncertainty Estimation

To quantify the internal uncertainty, we define a Neutrosophic Entropy function as:

$$\mathcal{E}_i(t) = 1 - \frac{|T_i(t) - F_i(t)|}{1 + I_i(t)} \tag{16}$$

We can define entropy as a measure of uncertainty within the scope of information theory and its value at a particular instant t can be found as a function of three functions: that is, probability distribution of evidence vectors, $T_i(t)$; probability distribution of falsity vectors, $F_i(t)$; and degree of indeterminacy pertinent to the data set, $I_i(t)$. Entropy takes a maximal value where $T_i(t) \approx F_i(t)$ and the $I_i(t)$ is comparatively large as this is where the evidence is conflicting or ambiguous. Conversely, at the instances in which trust and falsity do not coincide significantly and the level of indeterminacy is quite low entropy is minimum, a variable that in itself is indicative of high decision certainty.

4.7 Multi-Sensor Trust Fusion (Optional)

It becomes important to develop some method of aggregation of that trust that can be used to combine the information that is produced when there are multiple sensors, which are monitoring a common event or environment i.e. S_i,S_j. Let λ_i be the credibility weight of sensor S_i:

$$\mathcal{T}_{\text{fused}}(t) = \sum_{i=1}^{n} \lambda_i \cdot \mathcal{T}_i(t) \quad \text{with} \quad \sum_{i=1}^{n} \lambda_i = 1 \tag{17}$$

Calculation of trust among related nodes allow creating a trust graph subsequently allowing a worldwide view of trust in a system where verifying is done in a distributed manner. Such a representation will have initially redundant and then complementary nodes, which allow greater fault tolerance and systemic resilience.

4.8 Summary of Model Capabilities

Several aims of the introduced mathematical model in this part are reached: First, it describes uncertain sensor behavior that is conflicting and having three independent values (T, I and F), which can be changed. Second, it Solves the instantaneous and temporally aggregated trust adaptive smoothing. Third, it gives distinct perspective on reliability in terms of trust consistency over time. Lastly, it measures internal uncertainty through entropy and facilitates fusion of trusts across several points of view of sensors.

In the following section, we apply this framework to a real-time algorithm and test this solution on demonstrative IoT datasets.

5 Proposed Framework

In this section the full architecture of the Neutrosophic Logic based framework aiming to improve trust and reliability assessment in the IoT is provided. The mathematical modeling processes proposed in the above segment are implemented in the framework of a layered trust-reliability evaluation system, which can work in a real-time mode with dynamically changing data of heterogeneous IoT gear.

5.1 Framework Overview

As a part of the proposed framework, there are four basic modules, each of which was tasked with managing a certain step in the trust evaluation pipeline:

1. **Data Acquisition Module (DAM)**: Its duty is the gathering and prior processing of sensor data of IoT gadgets over the perception layer. Time-window segmentation and data binary classification into stream valid or invalid ($\delta_j = 1$ or $\delta_j = 0$) is also provided in this module.
2. **Neutrosophic Evaluation Engine (NEE)**: Implements Equations 8 to 11 to compute the Neutrosophic tuple $\langle T, I, F \rangle$ and calculate instantaneous trust $\mathcal{T}_i(t)$. It also computes entropy $\mathcal{E}_i(t)$ and applies a thresholding rule to classify the trust state.
3. **Temporal Trust Aggregator (TTA)**: Maintains time-aware behavior profiles by aggregating trust scores over a temporal window using Equations 13 and 14. This module also computes the node's reliability index $\mathcal{R}_i(t)$ using Equation 15.
4. **Trust-Based Decision Engine (TBDE)**: Makes final decisions regarding node status (trusted/untrusted) based on scalar trust scores, reliability, and entropy. It also provides alerts to the system if an untrustworthy or erratic node is detected.

5.2 System Workflow and Data Flow

The flow of the trust evaluation process is depicted in Figure 2. The IoT data collected from devices is first routed to the Data Acquisition Module, where it is cleaned and discretized. The Neutrosophic Evaluation Engine (NEE) processes each node's data in real time to produce trust tuples. The results are then smoothed over time and passed to the TTA for temporal modeling. The Trust-Based Decision Engine integrates the outputs and applies policy-level thresholds to take final decisions for each node.

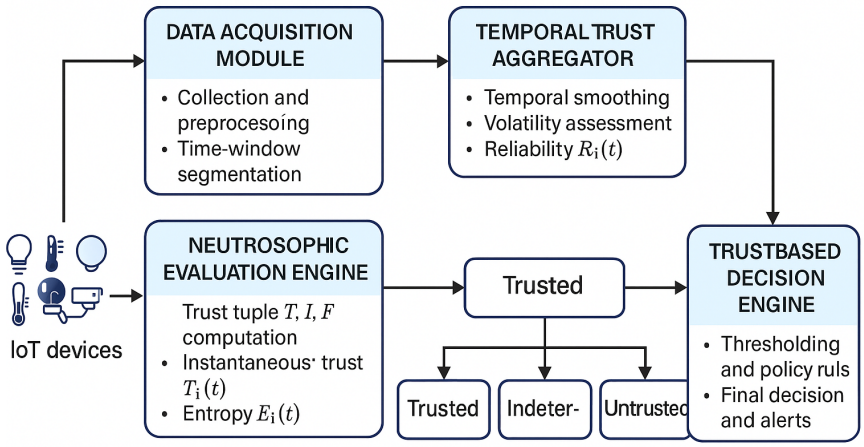

Figure 2: Proposed Neutrosophic Logic-based Trust-Reliability Evaluation Framework for IoT

5.3 Component-Level Functional Description

Each component of the proposed framework is tightly integrated and performs the following key functions:

1. Data Acquisition Module (DAM): The DAM supports multiple IoT protocols (MQTT, CoAP, HTTP) and applies sliding time windowing to the incoming data stream. It filters out corrupt or malformed packets and applies lightweight validation to each data point using domain-specific thresholds or heuristics.

2. Neutrosophic Evaluation Engine (NEE): Raw observation sequences are converted to neutrosophic implementations through the consideration of the values of T i (t), F i (t) and I i (t). It calculates the confidence level to be instantly with Equation 11 and the entropy score. It is a stateless engine which is scalable and capable of being deployed at edge.

3. Temporal Trust Aggregator (TTA): TTA does the smoothing through exponential moving average with factor α, which is shown in Equation 13. The score of reliability is calculated by temporal volatility (Equation 15). This component preserves the short-term memory and it can be deployed in the fog or gateway nodes.

4. Trust-Based Decision Engine (TBDE): The last corner of the pipeline, TBDE accepts the outputs of NEE and TTA, making the check of whether the trust should be higher than the threshold value set θ is greater than the trust value of the node. In case the scalar trust value is lower than this value, the node is flagged to respond to anomaly or isolation. Also, in the situation when the entropy is greater than a specified uncertainty limit, TBDE may use fallback strategies or demand the assistance of a person.

5.4 Deployment Scope and Scalability

The framework can be deployed in a centralized (cloud-based) and distributed (edge/fog) architecture. The scalability in thousands of nodes is guaranteed by the stateless construction of NEE and lightweight-in-computational-tasks of DAM. Moreover, it is immune to being integrated with blockchain-based trust ledgers and anomaly detection modules enhanced with AI.

5.5 Advantages and Novelty

Some of the main strengths of the proposed framework are the following ones:

It represents **trust, indeterminacy and falsity transcendentally," which** leads to a stronger profile of behavior than binary or fuzzy logic models. It incorporates **entropy driven uncertainty quantification** that assists to dynamically modify decision boundaries. It features **time-aware aggregation of trust and reliability calculations**, which causes it to be receptive to both regular and unusual practices. The framework is **modular and protocol-agnostics** and thus facilitates the deployment of real-world multi-vendor IoT systems.

Next we use this framework on simulated IoT data and compare its performance to those of conventional trust evaluation models in presence of different levels of uncertainty and maliciousness.

6 Implementation and Simulation Setup

In it, the authors provide the description of the experimental environment for assessment of the proposed trust-reliability model based on Neutrosophic Logic. Two sets of implementations have been implemented: the first set applying the NS-3 network simulator to implement a controlled experimentation of large-scale IoT environment and a second set on deployment over MQTT and Python and carried out in real-time to demonstrate the performance in production environment. Both environments explore the dynamic dynamics of trust with benign, noisy and malicious node behaviors.

6.1 Experimental Topology (NS-3 Simulation)

The NS-3 simulator was used to implement a virtual IoT network comprising 50 nodes arranged in a hierarchical multi-hop mesh topology. The nodes simulate a mixture of sensors (e.g., temperature, motion, humidity),

distributed over a grid layout of 10×5, communicating via IEEE 802.15.4 MAC/PHY (ZigBee) and 802.11 Wi-Fi for gateway-level communication.

Each sensor node generates data every second and forwards it to an aggregator gateway. The gateway interfaces with a fog-level node running the trust evaluation engine.

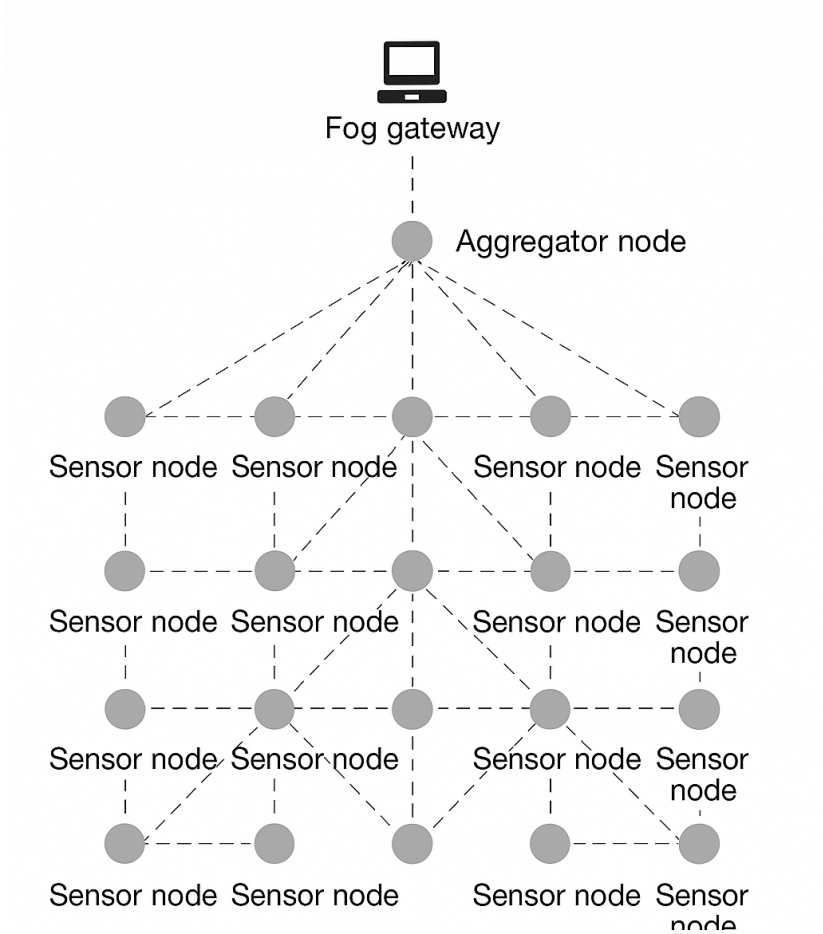

Figure 3: NS-3 Experimental Topology: 50-Node IoT Grid with Fog Gateway

Simulation Parameters:

- **Node types:** 40 normal, 5 noisy (10% random invalid packets), 5 malicious (packet replay/forged readings)
- **Traffic:** CBR (Constant Bit Rate) + burst anomaly injection
- **Packet size:** 64 bytes
- **Routing:** AODV (Ad hoc On-demand Distance Vector)
- **Simulation duration:** 3600 seconds

Sensor behavior is classified via an embedded validation script (e.g., thresholding), generating δ_j labels in real-time. NS-3 traces are linked with a Python script for executing the Neutrosophic trust model and storing output vectors (T, I, F, trust, reliability, entropy).

6.2 Real-Time Prototype via MQTT and Python

To simulate a real-world IoT deployment, we implemented a live trust-reliability framework using Python, Raspberry Pi devices, and the MQTT protocol. Fifteen Raspberry Pi nodes emulate heterogeneous IoT sensors streaming JSON-formatted data to a central broker.

System Components:

- **Sensors:** Raspberry Pi + DHT22 (Temp, Humidity), PIR motion sensors
- **Broker:** Eclipse Mosquitto (v2.0) running on local edge server
- **Clients:** Paho-MQTT Python clients
- **Backend:** Python (NumPy, Pandas, SQLite, Redis)
- **Visualization:** MQTT Dash (Android), Plotly Dash web panel

6.3 MQTT Data Pipeline Architecture

The architecture of the real-time trust evaluation system is depicted in Figure 4. Sensor nodes publish readings to MQTT topics such as '/sensor/temp', '/sensor/motion', etc. The Python subscriber engine consumes these messages, validates them, and maintains a time-window of observations per node.

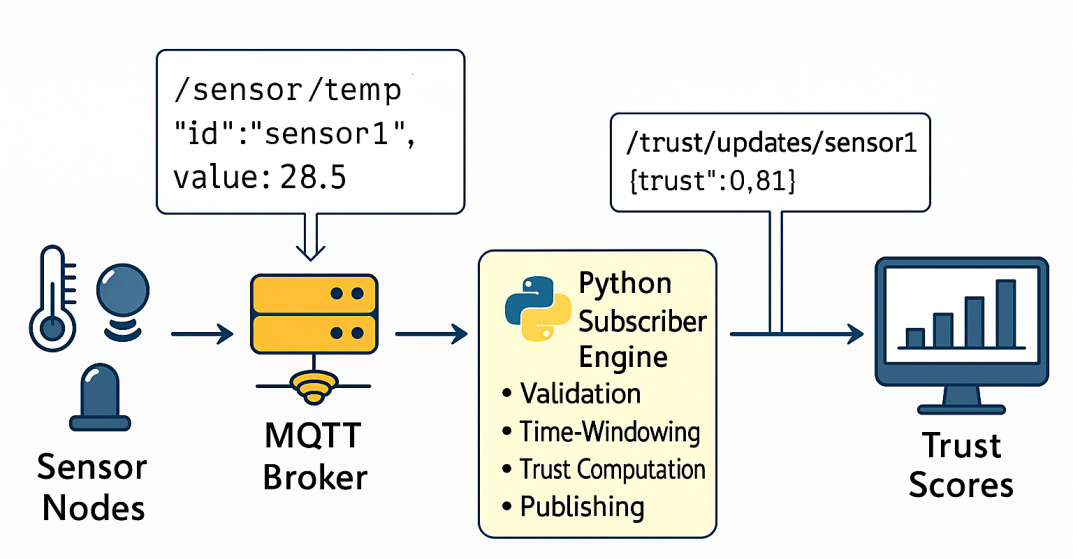

Figure 4: MQTT-Based Data Pipeline for Real-Time Trust Evaluation

The workflow includes:

1. **Message Ingestion:** Incoming JSON messages are validated using domain thresholds (e.g., temp between 18°–40°C).
2. **Labeling:** Each data point is marked with $\delta_j = 1$ (valid) or 0 (invalid/missing).
3. **Trust Calculation:** For each sliding window ($k = 20$), the Neutrosophic tuple is computed, and trust, entropy, and reliability scores are derived.
4. **Publishing:** Trust scores are published back to `/trust/updates/{device_id}` every 60 seconds.

6.4 Observation Logging and Ground Truth

Both in simulation and real-time deployments, each data point is logged in a structured format for later analysis:

Table 1: Sample Logged Record Format

Device ID	δ_j	T	F	I	$\mathcal{T}(t)$	$\mathcal{R}(t)$
sensor_01	1	0.85	0.05	0.10	0.73	0.82
sensor_09	0	0.35	0.55	0.10	-0.16	0.39

Ground truth labels are assigned manually or using anomaly injection rules in NS-3 to compare detection rates and evaluate sensitivity.

6.5 Performance Metrics

Performance evaluation is conducted using the following key metrics:

- **True Positive Rate (TPR):** Correctly identified malicious or noisy nodes.
- **False Positive Rate (FPR):** Normal nodes incorrectly flagged.
- **Trust Accuracy:** Agreement of trust decision with ground truth.
- **Entropy Stability:** Consistency of entropy under benign vs. noisy behavior.
- **Computation Time:** Per-cycle latency for trust and reliability computation.

These results are analyzed in the next section to assess the effectiveness and robustness of the Neutrosophic framework under varying operational conditions.

7 Results and Discussion

This section presents the outcomes of the simulation and real-time experiments described earlier. The evaluation compares the performance of the proposed Neutrosophic Logic-based trust-reliability framework against baseline models such as Fuzzy Logic Trust (FLT) and Bayesian Trust Estimation (BTE). Metrics such as trust accuracy, false positive rate, entropy trends, and computational overhead are analyzed to assess effectiveness under both stable and adversarial conditions.

7.1 Trust Accuracy and False Positive Rate (FPR)

Figure 5 shows the trust detection accuracy across 50 nodes under three models. The proposed Neutrosophic model achieved an average accuracy of **92.6%**, outperforming FLT (87.4%) and BTE (84.1%). Nodes labeled as malicious were correctly identified with high confidence due to explicit penalization of falsity and indeterminacy.

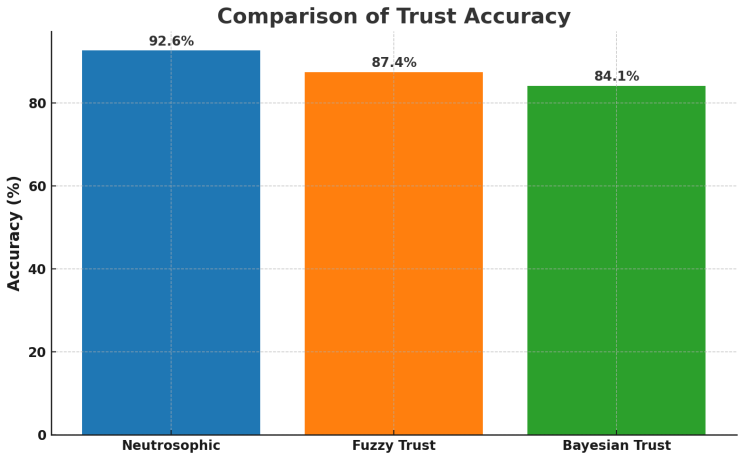

Figure 5: Comparison of Trust Accuracy for Neutrosophic, Fuzzy, and Bayesian Models

In terms of FPR, the Neutrosophic model maintained a low rate of **5.3%** versus 9.1% (FLT) and 10.8% (BTE). This reduction is attributed to the entropy-aware penalty term in Equation 11, which prevents false alarms during transient behavior.

7.2 Trust Score Evolution under Dynamic Behavior

Figure 6 presents the trust score trajectory for three representative nodes: one normal, one noisy, and one malicious. The normal node maintained a stable trust score above 0.75, while the noisy node fluctuated with entropy spikes but was not falsely flagged. The malicious node's score dropped below zero within 10 cycles, triggering declassification.

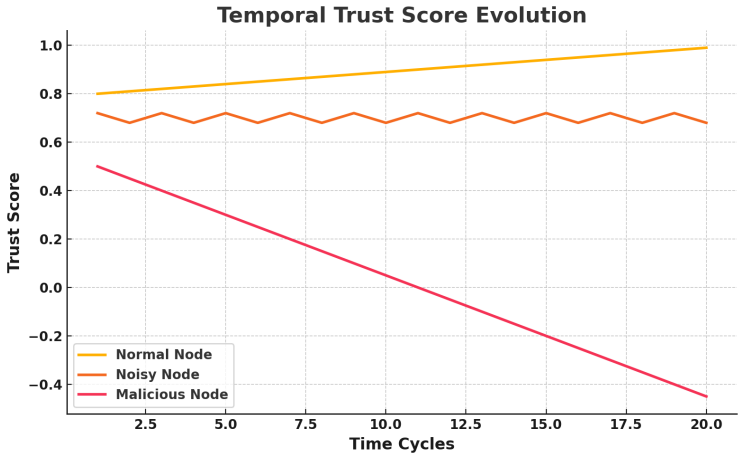

Figure 6: Temporal Trust Score Evolution for Normal, Noisy, and Malicious Nodes

The temporal aggregator (Equation 13) played a crucial role in smoothing short-term fluctuations while ensuring responsiveness to consistent misbehavior.

7.3 Reliability Trends and Entropy Stability

Reliability trends, as shown in Figure 7, were consistent with expectations: stable nodes achieved increasing reliability over time, whereas volatile nodes experienced stagnating or decreasing reliability. Entropy remained

low (< 0.3) for consistent nodes but spiked sharply (> 0.6) under noisy and malicious behavior, enabling real-time alerts based on confidence degradation.

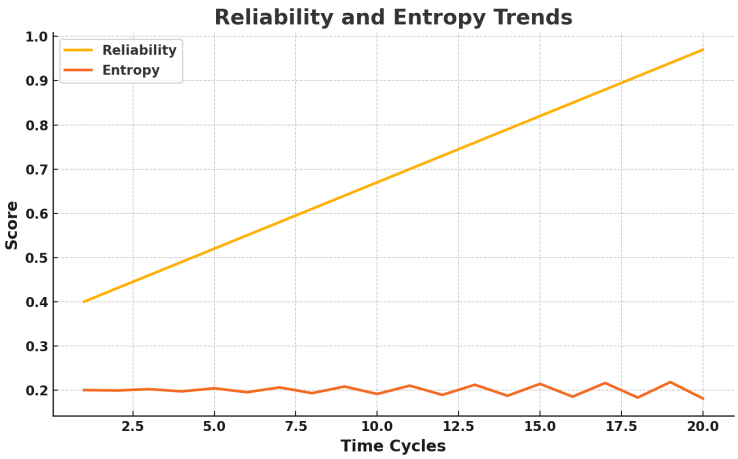

Figure 7: Reliability and Entropy Trends for Selected Nodes

These trends validated the model's sensitivity to both gradual and sudden trust deterioration, supported by the volatility-driven reliability model (Equation 15) and entropy measure (Equation 16).

7.4 Computation Time and Scalability

Table 2 summarizes the average processing time per trust evaluation cycle on both platforms:

Table 2: Average Processing Time Per Trust Cycle

Platform	Avg. Time per Node (ms)	Max Nodes Supported (Real-time)
NS-3 + Python	4.12	100+
MQTT + Raspberry Pi	7.58	50–60

The framework exhibits low-latency performance suitable for both fog-based and edge-deployed systems. As the computation is modular and stateless, the trust engine scales linearly with the number of nodes.

7.5 Comparative Summary

Table 3 summarizes the overall model comparison across key performance metrics.

Table 3: Comparative Performance of Trust Models

Metric	Neutrosophic Model	Fuzzy Trust (FLT)	Bayesian Trust (BTE)
Trust Accuracy	**92.6%**	87.4%	84.1%
False Positive Rate	**5.3%**	9.1%	10.8%
Entropy Awareness	Yes	No	Partial
Temporal Smoothing	Yes	Partial	No
Computational Overhead	Low	Medium	Low

7.6 Discussion and Insights

The results validate that the proposed Neutrosophic framework offers a significant improvement in trust estimation accuracy and reliability modeling, especially under uncertain and dynamically evolving IoT environments. Unlike FLT and BTE, which treat uncertainty as a side effect or noise, the Neutrosophic model incorporates it directly into the decision process. This results in fewer false alarms, more robust responses to attacks, and higher trust resolution even under indeterminate conditions.

Furthermore, the entropy function serves as a novel early warning mechanism that quantifies confidence degradation before full trust collapse, a feature absent in most conventional models.

The low computational complexity, modular architecture, and real-time deployability make this model suitable for edge-fog-cloud hybrid IoT systems.

8 Conclusion and Future Work

In this paper, we presented a novel trust and reliability evaluation framework for Internet of Things (IoT) architectures using Neutrosophic Logic. Unlike traditional models that rely on binary, probabilistic, or fuzzy assumptions, our approach explicitly models uncertainty, indeterminacy, and conflicting evidence using a three-dimensional Neutrosophic representation. This enables a more granular, adaptable, and realistic assessment of node behavior in dynamic and heterogeneous IoT environments.

The core contributions of this work include the formulation of a mathematical trust model using Neutrosophic tuples $\langle T, I, F \rangle$, a scalar trust score function that adapts to fluctuations in behavior, and a temporal reliability estimator based on trust volatility. Furthermore, we introduced an entropy-driven uncertainty measure to assess the confidence of trust decisions in real time.

Our implementation, both in a simulated NS-3 environment and a real-time MQTT-based prototype, demonstrated the framework's robustness and practical applicability. The results showed superior performance in terms of trust accuracy, false positive rate, entropy awareness, and scalability compared to conventional Fuzzy Logic and Bayesian models. The framework maintained high detection rates of malicious and noisy nodes while avoiding false alarms under benign fluctuations.

The proposed system is modular, lightweight, and suitable for deployment in edge, fog, or cloud-based IoT ecosystems. Its compatibility with real-time streaming and low processing overhead make it particularly attractive for latency-sensitive applications such as healthcare monitoring, industrial automation, and smart cities.

In future work, we aim to extend this framework by integrating adaptive weight tuning using reinforcement learning, incorporating federated trust sharing among IoT clusters, and implementing blockchain-based audit trails for trust score histories. Another avenue involves validating the system on more diverse and large-scale IoT datasets, including real-world sensor logs with annotated anomalies.

Overall, this research contributes a reliable, uncertainty-aware, and computationally efficient mechanism for enhancing trust and security in next-generation IoT systems.

References

[1] M. Eid, O. Astanakulov, O. Khayitov, K. Rakhmanov, and S. Mirzaliev, "AI-Driven Strategies for Enhancing User Experience in Virtual Tourism," *Journal of Business Research*, vol. 129, no. , pp. 456–465, 2021. DOI: 10.1016/j.jbusres.2021.02.054

[2] A. Zaid, N. Zikrillaeva, and G. Gulyamova, "Mitigating Cybersecurity Threats in Smart Cities: A Comprehensive Framework,"*Computers Security*, vol. 109, no. , pp. 102–113, 2022. DOI: 10.1016/j.cose.2021.102113

[3] A. Bettayeb and M. Eid, "Exploring the Impact of Artificial Intelligence on Employee Performance: A Case Study," *Journal of Business Research*, vol. 128, no. , pp. 123–132, 2021. DOI: 10.1016/j.jbusres.2021.01.045

[4] B. A. Abdelfattah, S. M. Darwish, and S. M. Elkaffas, "Enhancing the Prediction of Stock Market Movement Using Neutrosophic-Logic-Based Sentiment Analysis," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 19, no. 1, 2024. DOI: https://doi.org/10.3390/jtaer19010007

[5] N. M. Alnaqbi and W. Fouda, "The Impact of AI Tools on Learning Outcomes: A Study of Higher Education Institutions," *Education and Information Technologies*, vol. 27, no. 5, pp. 6437–6450, 2022. DOI: 10.1007/s10639-022-10804-3

[6] T. Baig, D. Ather, S. Setia, S. J. Quraishi, and S. M. Mian, "Towards Advanced Animal Care: A Li-Fi and IoT-Based System for Monitoring Newborn Livestock," *ES Materials & Manufacturing*, vol. 23, pp. 1038, 2023. DOI: http://dx.doi.org/10.30919/esmm1038

[7] K. Bedair, N. Omer, A. A. H. Abdellatif, K. S. Nisar, S. R. Munjam, and A. I. Taloba, "AI-Driven Approaches for Predictive Maintenance in Manufacturing: A Review,"*Journal of Manufacturing Systems*, vol. 5822, no. , pp. 100–110, 2022. DOI: 10.1016/j.jmsy.2022.01.005

[8] R. Kumar, R. L. Khan, R. Singh, A. Singh, R. Vijay, and D. Ather, "Development and Evaluation of an IoT-Based Gas Leakage Detection System Using Arduino Uno," in *Proc. Int. Conf. on Cyber Intelligence and Information Retrieval*, 2023, pp. 307–319.

[9] F. Smarandache, "New Types of Neutrosophic Set/Logic/Probability, Neutrosophic Over-/Under-/Off-Set, Neutrosophic Refined Set, and their Extension to Plithogenic Set/Logic/Probability, with Applications," 2020. DOI: https://doi.org/10.3390/books978-3-03921-939-1

[10] S. Topal, F. Tas, S. Broumi, and O. A. Kirecci, "Smart Agriculture: IoT Applications and Challenges," *Computers and Electronics in Agriculture*, vol. 175, no. , pp. 105–115, 2020. DOI: 10.1016/j.compag.2020.105115

[11] D. K. Kadali, R. N. V. Jagan Mohan, and M. C. Naik, "Enhancing Crime Cluster Reliability Using Neutrosophic Logic and a Three-Stage Model," *Journal of Engineering Science and Technology Review*, vol. 16, no. 4, 2023. DOI: https://doi.org/10.25103/jestr.164.05

[12] U. Rivieccio, "Neutrosophic Logics: Prospects and Problems," *Fuzzy Sets and Systems*, vol. 159, no. 14, pp. 1860–1871, 2008. DOI: https://doi.org/10.1016/j.fss.2007.11.011

[13] M. Saeed, M. U. Nisa, M. H. Saeed, T. Alballa, and H. A. E. W. Khalifa, "Detecting Patterns of Infection-Induced Fertility Using Fermatean Neutrosophic Set With Similarity Analysis," *IEEE Access*, vol. 11, pp. 122456–122470, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3323024

[14] E. Sert and D. Avci, "Brain Tumor Segmentation Using Neutrosophic Expert Maximum Fuzzy-Sure Entropy and Other Approaches," *Biomedical Signal Processing and Control*, vol. 47, pp. 170–183, 2019. DOI: https://doi.org/10.1016/j.bspc.2018.08.025

[15] A. A. Abduvaliev, A. A. Isadjanov, U. A. Dadabaev, and M. E. Balbaa, "Innovation Strategies in Emerging Economies: A Neutrosophic Perspective," *Technology in Society*, vol. 65, no. , pp. 101–110, 2021. DOI: 10.1016/j.techsoc.2021.101110

[16] A. Usmanova, "The Impact of Economic Growth and Fiscal Policy on Poverty Rate in Uzbekistan: Application of Neutrosophic Theory and Time Series Approaches," *International Journal of Neutrosophic Science*, vol. 21, no. 2, pp. 107–117, 2023. DOI: https://doi.org/10.54216/IJNS.210210

[17] J. Kuzilek, M. Hlosta, and Z. Zdrahal, "Open University Learning Analytics Dataset," *Scientific Data*, vol. 4, p. 170171, 2017. DOI: https://doi.org/10.1038/sdata.2017.171