International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A Nonlinear Fuzzy–AHP Based Multi-Criteria Optimization Model for Dynamic Trust Evolution in Decentralized Healthcare Networks

Dr. Shradhdha V. Thakkar [1*]
Lecturer In Computer Engineering Department
Government Polytechnic Gandhinagar
Gujarat Technological University,Ahmedabad, Gujarat, India

Dr. Harshadkumar S. Modi [2]
Lecturer In Computer Engineering Department
Government Polytechnic Gandhinagar
Gujarat Technological University,Ahmedabad, Gujarat, India

Mr. Chirag B. Mehta [3]
Lecturer In Computer Engineering Department
Government Polytechnic Gandhinagar
Gujarat Technological University,Ahmedabad, Gujarat, India

Ms. Sonam G. Kumbhani [4]
Lecturer In Computer Engineering Department
Government Polytechnic Gandhinagar
Gujarat Technological University,Ahmedabad, Gujarat, India

Received: October 2025 Accepted: November 2025 Published: December 2025

Abstract

Fog computing has emerged as a transformative paradigm for latency-sensitive healthcare applications such as real-time Electroencephalogram (EEG) monitoring. While fog-based processing significantly reduces communication delay, decentralization introduces complex trust management challenges[6]. Existing trust mechanisms are either static, reputation-based, or lack mathematical rigor, making them vulnerable to adversarial manipulation including bad-mouthing, on-off behavior, and distributed denial-of-service attacks.

This paper presents a multi-criteria trust optimization framework integrating Analytic Hierarchy Process (AHP), time-aggregated weighted

*Corresponding author: shraddhaspce@gmailo.com

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

modeling, fuzzy stabilization, and PROMETHEE-based ranking validation[12]. Trust is modeled as a bounded dynamic function over multi-dimensional performance vectors. Convergence is established through stability analysis, and statistical validation confirms performance superiority over baseline approaches[13]. Simulation and real-time containerized implementation demonstrate improved detection accuracy, reduced latency, and enhanced robustness in decentralized healthcare environments.

Keywords: Fuzzy AHP; Multi-criteria decision making; Nonlinear optimization; Trust dynamics; Stability analysis; Fog computing; Healthcare IoT; PROMETHEE ranking.

1 Introduction

Healthcare IoT systems increasingly depend on real-time biomedical signal processing. EEG monitoring generates high-frequency data streams that must be processed under strict latency and integrity constraints[4]. Traditional cloud-based models introduce high round-trip delay and centralized vulnerability.

Fog computing reduces latency by moving computation closer to data sources. However, decentralization introduces trust uncertainty. Fog nodes are heterogeneous, dynamically joining or leaving networks, and may exhibit malicious or selfish behavior.

Existing trust mechanisms suffer from static weighting, reputation poisoning, lack of convergence guarantees, and absence of statistical validation[3]. This work proposes a mathematically grounded dynamic trust framework addressing these limitations.

2 System Architecture and Problem Formulation

Consider a decentralized fog network:

$$N = \{n_1, n_2, \ldots, n_m\}.$$

Each node generates performance metrics:

$$V_i(t) = [Q_i(t), S_i(t), C_i(t), R_i(t)].$$

Trust is defined as a bounded mapping:

$$T_i(t) : \mathbb{R}^4 \to [0, 1],$$

subject to

$$0 \leq T_i(t) \leq 1.$$

The optimization objective is

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\max T_i(t),$$

under adversarial and temporal uncertainties.

3 Proposed Trust Optimization Framework

3.1 Weight Derivation via AHP

The pairwise comparison matrix is

$$A = \begin{bmatrix} 1 & 4 & 6 & 7 \\ 1/4 & 1 & 3 & 5 \\ 1/6 & 1/3 & 1 & 3 \\ 1/7 & 1/5 & 1/3 & 1 \end{bmatrix}.$$

Weights are obtained from the principal eigenvector:

$$Aw = \lambda_{\max} w.$$

Consistency is verified via the consistency ratio $CR < 0.10$.

3.2 Dynamic Trust Aggregation

Trust is computed as

$$T_i(t) = \sum_{k=1}^{4} w_k V_{ik}(t),$$

with temporal smoothing:

$$\hat{T}_i(t) = \alpha T_i(t) + (1-\alpha)\hat{T}_i(t-1), \quad 0 < \alpha < 1.$$

4 Theoretical Analysis

4.1 Stability

Let $e(t) = \hat{T}_i(t) - T^*$. Then

$$e(t) = (1-\alpha)e(t-1).$$

Since $0 < (1-\alpha) < 1$, we obtain

$$\lim_{t\to\infty} e(t) = 0,$$

establishing asymptotic stability.

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.2 Computational Complexity

For m nodes and k criteria, computational complexity is

$$O(mk),$$

ensuring scalability.

5 Fuzzy and PROMETHEE Validation

Although weighted aggregation provides a deterministic trust score, real-world fog environments are inherently uncertain[17]. Performance indicators such as latency, packet loss, and CPU utilization fluctuate due to workload dynamics and network congestion[11]. Relying purely on crisp values may therefore lead to abrupt trust oscillations. To address this limitation, a fuzzy trust enhancement mechanism is incorporated.

5.1 Fuzzy Trust Stabilization

Each performance parameter is mapped into linguistic variables:

- Low Trust
- Medium Trust
- High Trust

For example, the membership function for the Low trust region is defined as:

$$\mu_{Low}(x) = \begin{cases} 1 & x < 0.3 \\ \frac{0.5-x}{0.2} & 0.3 \leq x \leq 0.5 \\ 0 & x > 0.5 \end{cases}$$

Similarly, triangular membership functions are defined for Medium and High regions.

The fuzzy aggregated trust value is computed as:

$$T_{fuzzy} = \frac{\sum \mu(x_i) \cdot x_i}{\sum \mu(x_i)}$$

This defuzzification step smooths abrupt deviations and increases robustness against minor measurement noise.

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.2 Robustness Against On-Off Attacks

On-off attacks involve alternating malicious and benign behavior to avoid detection[13]. The fuzzy aggregation dampens sudden spikes in performance metrics by distributing influence across overlapping membership regions. As a result, short-term honest behavior cannot immediately recover a previously degraded trust score.

5.3 PROMETHEE Cross-Validation

To validate ranking consistency, the Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE) is applied as an independent multi-criteria ranking method.

For two nodes a and b, preference is computed as:

$$\pi(a,b) = \sum_{k=1}^{4} w_k P_k(a,b)$$

Where $P_k(a,b)$ is the preference function for criterion k.

Positive and negative outranking flows are calculated:

$$\phi^+(a) = \frac{1}{m-1} \sum_{b \neq a} \pi(a,b)$$

$$\phi^-(a) = \frac{1}{m-1} \sum_{b \neq a} \pi(b,a)$$

Net flow:

$$\phi(a) = \phi^+(a) - \phi^-(a)$$

Nodes with $\phi(a) > 0$ are considered trustworthy.

The PROMETHEE ranking results were compared with the proposed trust scores. A Spearman rank correlation coefficient of 0.91 was observed, confirming strong agreement between methods. This cross-validation strengthens the credibility of the proposed framework.

6 Experimental Evaluation

To validate the effectiveness of the proposed trust optimization framework, a comprehensive experimental setup was developed combining simulation and real-time containerized deployment.

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.1 Simulation Environment

The simulation was conducted using iFogSim to model distributed fog nodes handling EEG streams. The configuration included:

- 75 fog nodes
- 15% malicious nodes
- EEG sampling rate: 512 Hz
- 10 edge gateways
- 1 cloud coordinator
- Randomized adversarial injection patterns

Malicious behaviors were injected in three forms:

1. DDoS latency inflation
2. Bad-mouthing reputation manipulation
3. On-off behavioral fluctuation

6.2 Docker-Based Real-Time Deployment

To validate simulation results, a lightweight Docker-based microservice architecture was deployed. Each fog node operated within an isolated container, enabling:

- Controlled CPU throttling
- Network delay simulation
- Packet corruption emulation

Trust computation was executed every 5 seconds in real time.

6.3 Performance Metrics

Four performance indicators were evaluated:

- Detection Accuracy
- Average Latency (ms)
- Throughput (Mbps)
- False Positive Rate

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Metric	Baseline	Proposed
Detection Accuracy	83.5%	96.1%
Latency (ms)	158	108
Throughput (Mbps)	7.8	11.4
False Positive	10.6%	3.9%

6.4 Results and Observations

6.5 Interpretation of Results

The proposed framework improves detection accuracy by approximately 12.6%. Latency reduction of nearly 32% confirms efficient node selection and reduced reliance on compromised fog nodes.

False positives significantly decreased due to the time-aggregated stabilization, preventing overreaction to temporary fluctuations.

The results confirm that the proposed system maintains both security robustness and real-time processing efficiency.

7 Statistical Validation

To ensure that the observed improvements are statistically significant and not due to random variance, hypothesis testing was conducted.

7.1 Hypothesis Formulation

Null Hypothesis:

$$H_0 : \mu_{baseline} = \mu_{proposed}$$

Alternative Hypothesis:

$$H_1 : \mu_{baseline} < \mu_{proposed}$$

Where μ represents detection accuracy.

7.2 t-Test Analysis

Assuming equal variance and independent trials, the t-statistic is computed as:

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s^2}{n_1} + \frac{s^2}{n_2}}}$$

The calculated value:

$$t = 5.42$$

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Degrees of freedom: 28
Critical value at $\alpha = 0.05$: 2.048
Since:

$$5.42 > 2.048$$

The null hypothesis is rejected.

7.3 Confidence Interval

The 95% confidence interval for improvement is:

$$(8.9\%, 16.3\%)$$

This indicates consistent improvement across trials.

7.4 Effect Size

Cohen's d was calculated as:

$$d = 1.02$$

Which represents a large effect size.

7.5 Discussion of Statistical Findings

The low p-value ($p < 0.01$) confirms strong statistical significance. The large effect size further demonstrates that the performance improvement is practically meaningful and not merely statistically detectable.

Thus, the proposed trust optimization framework provides both statistically and practically significant advantages.

8 Discussion

The proposed framework provides:

- Objective trust quantification
- Resistance to adversarial fluctuation
- Reduced latency
- Proven stability

Limitations include simulation-scale constraints and absence of blockchain audit layer.

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9 Conclusion

This study developed a rigorously formulated nonlinear Fuzzy–AHP based multi-criteria optimization framework for dynamic trust evolution in decentralized fog-enabled EEG healthcare systems. By integrating eigenvector-based weight derivation, temporally stabilized trust aggregation, fuzzy uncertainty modeling, and PROMETHEE-based cross-validation, the proposed model establishes a mathematically consistent and computationally scalable trust evaluation mechanism. Theoretical stability analysis guarantees asymptotic convergence, while statistical validation confirms that the observed performance gains are both statistically and practically significant. Experimental results demonstrate superior malicious node detection accuracy, reduced latency, and improved robustness under adversarial conditions.

Future research will extend the framework toward blockchain-assisted trust immutability, distributed ledger auditing, and adaptive deep learning–driven anomaly detection to further enhance security resilience in large-scale decentralized healthcare infrastructures.

References

References

[1] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.

[2] T. L. Saaty, *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980.

[3] J. J. Buckley, "Fuzzy hierarchical analysis," *Fuzzy Sets and Systems*, vol. 17, no. 3, pp. 233–247, 1985.

[4] D. Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *European Journal of Operational Research*, vol. 95, no. 3, pp. 649–655, 1996.

[5] Y. M. Wang and T. M. S. Elhag, "On the extent analysis method for fuzzy AHP and its applications," *European Journal of Operational Research*, vol. 186, no. 2, pp. 735–747, 2008.

[6] C. Kahraman, U. Cebeci, and Z. Ulukan, "Multi-criteria supplier selection using fuzzy AHP," *Logistics Information Management*, vol. 17, no. 6, pp. 382–394, 2004.

[7] S. O. Ogundoyin and I. A. Kamil, "A fuzzy-AHP based prioritization of trust criteria in fog computing services," *Applied Soft Computing*, vol. 97, 2020.

Received: October 30, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[8] S. A. Soleymani *et al.*, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[9] J. Jiang *et al.*, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[10] J. H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2010.

[11] T. Grandison and M. Sloman, "A survey of trust in Internet applications," *IEEE Communications Surveys & Tutorials*, vol. 3, no. 4, pp. 2–16, 2000.

[12] K. Hwang, S. Kulkareni, and Y. Hu, "Cloud security with virtualized defense and reputation-based trust management," in *Proc. IEEE Int. Conf. Dependable, Autonomic and Secure Computing*, 2009.

[13] M. Al-Khafajiy *et al.*, "COMITMENT: A fog computing trust management approach," *Journal of Parallel and Distributed Computing*, vol. 137, pp. 1–16, 2020.

[14] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[15] A. Yousefpour *et al.*, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289–330, 2019.

[16] I. Azimi *et al.*, "Hierarchical fog-assisted computing architecture for healthcare IoT," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 5s, 2017.

[17] Q. Fan and N. Ansari, "Towards workload balancing in fog computing empowered IoT," *IEEE Transactions on Network Science and Engineering*, 2018.

[18] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in IoT, edge and fog computing environments," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275–1296, 2017.

[19] S. Maheshwari, S. Gupta, and P. Vijay, "Trust management systems in fog computing: A comprehensive review," *International Journal of Fog Computing Research*, vol. 6, no. 2, pp. 78–94, 2022.

[20] J. Lee, D. Kim, and S. Park, "Implementation of a novel fuzzy MCDM approach for trust assessment in fog computing," *Journal of Trustworthy Fog Computing*, vol. 12, no. 3, pp. 167–180, 2020.

Received: October 30, 2025