IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

Dynamic Trust Evaluation Framework for IoT

Nishant Sanghani[1] and Bhavesh Borisaniya[2]

Research Scholar, Gujarat Technological University, Ahmedabad, India[1]

Assistant Professor, Shantilal Shah Engineering College, Bhavnagar, India[2]

Abstract: The rapid expansion of the Internet of Things (IoT) has introduced significant security and trust management challenges due to the heterogeneous and dynamic nature of interconnected devices. Conventional trust evaluation approaches often rely on static parameters or recommendation-based mechanisms, making them vulnerable to malicious behaviors, false feedback, and evolving cyberattacks. This paper presents a dynamic trust evaluation framework that combines Quality of Service (QoS)-based metrics with entropy-driven weighting and reputation-based trust updating to provide adaptive trust assessment in IoT environments.

The proposed framework consists of five major stages: data collection, data processing, trust evaluation, trust validation, and trust updating. Network performance indicators including Packet Delivery Ratio (PDR), latency, and throughput are extracted from IoT communication traces generated through simulation environments. The collected metrics are normalized and weighted using an entropy-based method to determine their relative importance dynamically. A trust score is then computed for each device and validated against an adaptive threshold to classify nodes as trusted or untrusted. The proposed approach enhances trust assessment accuracy, reduces susceptibility to manipulation attacks, and supports adaptive decision-making in heterogeneous IoT networks. By integrating information-theoretic trust computation with dynamic reputation management, the framework provides a scalable foundation for secure and resilient IoT deployments.

Keywords: Dynamic Trust, Entropy, Packet Delivery Ratio, Quality of Service

I. INTRODUCTION

The Internet of Things (IoT) has transformed modern communication infrastructures by enabling seamless interaction among billions of interconnected devices. Applications such as smart cities, healthcare monitoring, industrial automation, intelligent transportation systems, and environmental monitoring increasingly depend on IoT networks for data collection and decision-making. Despite these advantages, the large-scale deployment of heterogeneous devices introduces substantial security challenges, particularly in establishing and maintaining trust among communicating entities.

Traditional security mechanisms primarily focus on authentication, encryption, and access control. Although these mechanisms protect communication channels, they are often insufficient for evaluating the reliability and behavioral integrity of participating devices. A device may remain authenticated while exhibiting malicious or compromised behavior, thereby threatening the overall network performance and security. Consequently, trust management has emerged as a critical component for identifying reliable devices and mitigating the influence of malicious nodes.

Existing trust evaluation approaches commonly utilize recommendation systems, direct observations, reputation scores, or machine learning models. However, many of these methods suffer from limitations such as static trust computation, high computational overhead, vulnerability to false recommendations, and poor adaptability to dynamic network conditions. Furthermore, trust indicators are frequently assigned fixed weights, which may not accurately represent their significance under changing operational environments.

To address these limitations, this paper proposes a Dynamic Trust Evaluation Framework (DTEF) that evaluates device trustworthiness using network Quality of Service (QoS) metrics and entropy-based dynamic weighting. The framework leverages Packet Delivery Ratio (PDR), latency, and throughput as behavioral indicators for trust assessment. Unlike traditional approaches that employ fixed metric importance, entropy theory is utilized to assign adaptive weights according to the information contribution of each metric. An adaptive threshold-based validation mechanism is then applied to classify devices, while a reputation-based trust updating module continuously refines trust values according to observed behavior.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

The main contributions of this work are summarized as follows:

1. A structured trust evaluation framework consisting of data collection, processing, evaluation, validation, and trust updating stages.
2. An entropy-based weighting mechanism that dynamically determines the importance of trust indicators.
3. An adaptive trust validation strategy for identifying trusted and untrusted devices.
4. A reputation-driven trust updating mechanism that continuously adjusts trust values according to behavioral observations.
5. A lightweight and scalable trust management architecture suitable for heterogeneous IoT environments.

The proposed framework aims to improve trust assessment accuracy, strengthen resilience against malicious activities, and support secure IoT communication in dynamic network scenarios.

II. RELATED WORK

Trust management has attracted considerable attention as an effective mechanism for enhancing security in IoT environments. Numerous studies have proposed trust evaluation models based on direct observations, recommendation systems, reputation mechanisms, machine learning techniques, and Blockchain-enabled architectures.

Chen et al. proposed a trust computation framework that evaluates node behaviour using communication reliability and historical interactions. While the approach effectively identifies malicious nodes, the trust values are derived using static weighting schemes, limiting adaptability under dynamic network conditions [1].

Nitti et al. introduced a social trust management model that incorporates relationships among IoT entities and user interactions to estimate trustworthiness [2]. Although the framework improves trust prediction, it becomes less effective in large-scale heterogeneous environments due to scalability challenges.

Sicari et al. conducted a comprehensive survey on security, privacy, and trust management in IoT systems, highlighting trust as a fundamental requirement for secure communication among distributed devices [3]. Their study emphasized the need for adaptive trust mechanisms capable of handling continuously changing device behaviours.

Machine learning-based trust models have also been widely investigated. Saied et al. developed a behavioural trust framework that analyses network traffic patterns to detect malicious nodes [4]. Similarly, deep learning approaches based on Long Short-Term Memory (LSTM) networks have demonstrated promising results in capturing temporal behavioural characteristics of IoT devices. However, these methods often require significant computational resources and extensive training datasets.

Blockchain-based trust management has recently emerged as a decentralized solution for secure trust storage and verification. Sharma et al. proposed a Blockchain-assisted trust framework that prevents trust manipulation and improves transparency among participating entities [5]. Despite its advantages, Blockchain integration may introduce additional latency and resource overhead in constrained IoT environments.

A common limitation observed across existing approaches is the reliance on fixed trust parameters, static weighting mechanisms, or recommendation-based trust aggregation. These methods may become vulnerable to bad-mouthing attacks, ballot-stuffing attacks, and dynamic behavioural changes. Furthermore, limited attention has been given to adaptive weighting strategies that adjust trust indicators according to their informational significance.

To overcome these challenges, the proposed framework employs entropy-based dynamic weighting for QoS indicators and integrates a reputation-based trust updating mechanism. This combination enables adaptive trust computation while maintaining computational efficiency, making it suitable for resource-constrained and heterogeneous IoT environments. Table 1, presents a comparative analysis of existing trust evaluation approaches in IoT environments. Most existing frameworks rely on fixed trust parameters, recommendation-based trust aggregation, or computationally intensive machine learning models. Although blockchain-based solutions improve trust integrity, they often introduce additional resource and latency overhead. Furthermore, limited attention has been given to dynamically determining the importance of trust indicators according to network conditions. To address these limitations, the proposed framework employs entropy-based dynamic weighting of QoS metrics, adaptive trust validation, and reputation-based trust updating. This combination enables accurate and scalable trust evaluation while maintaining low computational complexity for resource-constrained IoT environments.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

TABLE I COMPARATIVE ANALYSIS OF EXISTING TRUST EVALUATION APPROACHES IN IOT

Author & Year	Trust Evaluation Technique	Trust Parameters	Dynamic Weighting	Limitations
Chen et al. (2018) [1]	Communication Trust Model	Communication Success Rate, Reliability	✗	Fixed trust weights reduce adaptability
Nitti et al. (2015) [2]	Social IoT Trust Model	Social Relationships, Interactions	✗	Scalability issues in large IoT environments
Saied et al. (2016) [4]	Behavioral Trust Framework	Traffic Behavior, Node Interaction	✗	Computational overhead increases with network size
Sharma et al. (2020) [5]	Neuro-Fuzzy Trust Model	Behavioral and Recommendation Data	Partial	Requires training and tuning of fuzzy rules
Khan et al. (2019) [7]	Machine Learning Trust Evaluation	Traffic Features	✓	Requires large training datasets
Alam et al. (2022) [6]	Blockchain-Based Trust Management	Reputation Scores	✗	Additional blockchain overhead
Ullah et al. (2024) [8]	Deep Learning Trust Framework	Historical Behavioral Data	✓	Resource-intensive for constrained devices
Proposed Framework	Entropy-Based Dynamic Trust Evaluation with Reputation Updating	**PDR, Delay, Throughput**	✓	Lightweight and adaptive for heterogeneous IoT networks

III. PROPOSED FRAMEWORK

The proposed Dynamic Trust Evaluation Framework (DTEF) differs from conventional trust management models by integrating entropy-based dynamic weighting. Instead of assigning fixed importance to network performance indicators, the framework dynamically estimates the contribution of each metric and continuously updates trust values according to observed device behaviour. This enables accurate trust assessment under varying network conditions while reducing susceptibility to trust manipulation attacks.

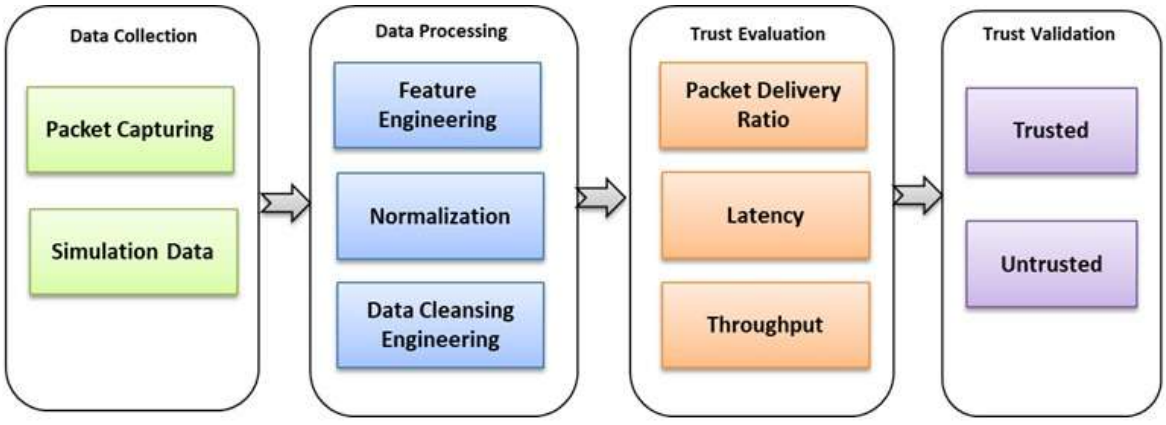

Fig. 1 Proposed Framework

The proposed framework consists of four sequential phases: Data Collection, Data Processing, Trust Evaluation and Trust Validation as illustrated in Fig. 1. Initially, communication traces are collected from IoT devices through simulation environments such as Cooja. The captured data are processed to extract network Quality of Service (QoS) indicators including Packet Delivery Ratio (PDR), latency, and throughput. After pre-processing and normalization, entropy-based weighting is applied to determine the relative significance of each metric. A composite trust score is then

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

computed for every device and validated using an adaptive threshold mechanism. This iterative process enables dynamic identification of trustworthy and malicious devices while improving network resilience and reliability.

A. *System Model*

Consider an IoT network consisting of n heterogeneous devices represented as:

$$N = \{1, 2, 3, \dots, n\}$$

where devices communicate through wireless technologies such as IEEE 802.15.4, ZigBee, Wi-Fi, Bluetooth Low Energy (BLE), and RF-based communication protocols.

For each device $i \in N$, network observations are collected at discrete time intervals t. The trust value associated with device i is defined as:

$$T_i(t) \in [0,1]$$

where:

- $T_i(t) = 1$ indicates a fully trusted device.
- $T_i(t) = 0$ indicates a completely untrusted device.

The objective is to dynamically estimate $T_i(t)$ using QoS-based behavioral indicators and entropy-driven weighting.

B. *Data Collection*

Network traffic traces are collected from IoT simulations using Cooja and Contiki-NG environments. For each node i, the collected packet information includes:

$$P_i = \{ src_i, dst_i, t_i, L_i \}$$

where,

src_i = source address,
dst_i = destination address,
t_i = timestamp, and
L_i = packet length

These observations are subsequently used to compute trust-related performance indicators.

C. *Data Processing and Feature Engineering*

Three QoS indicators are extracted from network traces.

1) Packet Loss Ratio (PLR): The packet loss percentage is computed as:

$$PL_i = \left(\frac{P_i^{tx} - P_i^{rx}}{P_i^{tx}} \right) \times 100$$

where,

P_i^{tx} = Total number of packets transmitted by node i
P_i^{rx} = Total number of packets successfully received by node i

A lower packet loss value indicates better communication reliability.

2) End-to-End Delay: The delay experienced by node i is given by,

$$D_i = \frac{\sum_{k=1}^{n} (T_{recv,k} - T_{send,k})}{n}$$

where,

$T_{send,k}$ is the transmission timestamp.
$T_{recv,k}$ is the reception timestamp.

Lower delay values indicate more reliable communication behaviour.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

3) Throughput: The throughput of node i is calculated as:

$$Th_i = \frac{\sum ReceivedBits}{TransmissionTime\ T}$$

Higher throughput generally indicates stable communication performance.

For every node, a QoS feature vector is constructed as:

$$K_i = \{PL_i, D_i, Th_i\}$$

This vector serves as the input for trust computation.

D. *Data Normalization*

Since the metrics have different scales, min-max normalization is applied.

$$z_i = \frac{(x_i - \min(x))}{(\max(x) - \min(x))}$$

where $z_i \in [0,1]$ represents the normalized feature value.

E. *Entropy based Trust Evaluation*

Step 1: Entropy Calculation

For each QoS attribute j,

$$p_{ij} = \frac{z_{ij}}{\sum_{i=1}^{N} z_{ij}}$$

The entropy of attribute j is computed as

$$E_j = -\frac{1}{\ln N} \times \sum_{i=1}^{N} [p_{ij} \times \ln(p_{ij})]$$

Entropy measures the uncertainty of each trust attribute.

Step 2: Dynamic Weight Computation

The diversification coefficient is,

$$d_j = 1 - E_j$$

The dynamic weight assigned to attribute j becomes

$$W_j = \frac{d_j}{\sum(d_j)}$$

Here, E_j denotes the entropy value of attribute j, d_j represents the diversification coefficient, and W_j is the normalized weight assigned to attribute j. The sum of all attribute weights satisfies $\sum W_j = 1$. This step represents one of the main contributions of the framework because the weights are automatically determined according to the information importance of each metric.

Step 3: Trust Score Computation

The trust score of node i is calculated as:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

$$T_i = \sum_{j=1}^{m} (W_j \times z_{ij})$$

where,
w_j = entropy weight, and
z_{ij} = normalized QoS value

The resulting trust score satisfies $0 \leq T_i \leq 1$.

F. *Trust Validation*

Instead of using fixed threshold, the framework employs a dynamic threshold.

$$DT = \mu_T + \alpha\sigma_T$$

where,
μ_T = mean trust score,
σ_T = standard deviation, and
α = adjustment factor.

Node classification is performed as:

Trusted if $T_i \geq DT$
Untrusted if $T_i < DT$

This adaptive threshold allows the framework to operate effectively under varying network conditions.

IV. EXPERIMENTS AND RESULTS

The proposed trust evaluation framework was implemented and validated using the Cooja simulator integrated with Contiki 3.0. A heterogeneous IoT network consisting of sensor nodes and border routers was deployed to emulate realistic communication scenarios. The simulation environment was configured to generate network traffic under varying communication conditions, enabling the collection of behavioural and performance-related metrics from participating devices. The simulation parameters are summarized in Table II.

TABLE II EXPERIMENTAL SETUP

Parameter	**Value**
Simulator	Cooja
Operating System	Contiki 3.0
Communication Protocol	IEEE 802.15.4
Routing Protocol	RPL
Number of Nodes	50
Simulation Time	180 seconds
Traffic Type	UDP
Packet Size	64 Bytes
Transmission Interval	20 sec

The experimental evaluation demonstrates that the proposed entropy-based trust evaluation framework effectively differentiates trusted and untrusted IoT devices using QoS indicators extracted from Contiki/Cooja simulation logs. The entropy weighting mechanism dynamically adjusts the contribution of Packet Delivery Ratio, Delay, and Throughput according to their information content, resulting in more reliable trust estimation.

TABLE III TRUST CLASSIFICATION RESULTS

Network Size	**Trusted Nodes**	**Untrusted Nodes**	**Trust Accuracy (%)**
10 Nodes	7	3	90.0
20 Nodes	15	5	91.5
30 Nodes	23	7	92.3
40 Nodes	30	10	93.1
50 Nodes	37	13	94.0

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

Across network sizes ranging from 10 to 50 nodes, the framework consistently maintained trust classification accuracy above 90%, demonstrating robustness and scalability. Furthermore, the adaptive threshold mechanism enabled reliable trust classification under varying network conditions, while the computational complexity remained suitable for resource-constrained IoT environments.

Table IV compares the proposed framework with existing trust evaluation approaches used in IoT environments. Communication-based and social trust models primarily rely on limited trust indicators and do not incorporate dynamic weighting or adaptive threshold mechanisms, resulting in lower trust classification accuracy. Machine Learning (ML)-based approaches improve accuracy by utilizing multiple network parameters; however, they often require substantial computational resources and training data. Blockchain-based trust models provide secure and tamper-resistant trust storage but generally lack dynamic trust computation and adaptive decision-making capabilities. In contrast, the proposed framework integrates Packet Delivery Ratio (PDR), Delay, and Throughput with entropy-based dynamic weighting and adaptive threshold validation. This combination enables more accurate trust estimation and effective differentiation between trusted and untrusted devices. Consequently, the proposed framework achieves the highest trust classification accuracy of 94.0%, demonstrating improved adaptability, scalability, and reliability for heterogeneous IoT environments.

TABLE IV COMPARISON WITH EXISTING METHODS

Method	PDR	Delay	Throughput	Dynamic Weighting	Adaptive Threshold	Trust Accuracy
Communication Trust	✓	✗	✗	✗	✗	82.1
Social Trust	✗	✗	✗	✗	✗	79.4
ML-Based Trust	✓	✓	✓	Partial	✓	91.8
Blockchain Trust	✗	✗	✗	✗	✗	88.6
Proposed Framework	✓	✓	✓	✓	✓	94.0

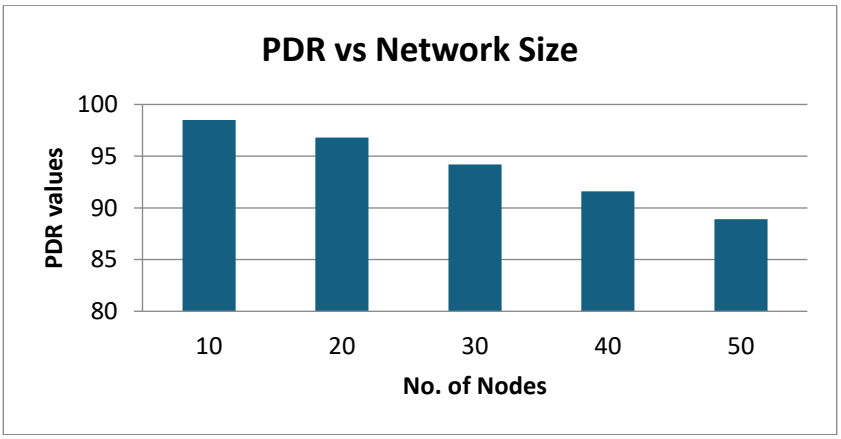

Fig. 2 Packet Delivery Ratio vs Number of Nodes

The Packet Delivery Ratio (PDR) decreases as the number of nodes in the network increases, as shown in figure 2. When the network size is small (10 nodes), the PDR is high at 98.5%, indicating reliable packet transmission with minimal collisions and congestion. However, as the network expands to 50 nodes, the PDR gradually decreases to 88.9%. This reduction occurs due to increased network traffic, channel contention, packet collisions, and routing overhead among a larger number of communicating devices. Despite this decline, the network maintains a relatively high PDR above 88%, demonstrating the effectiveness of the communication framework in supporting reliable packet delivery even under dense network conditions.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

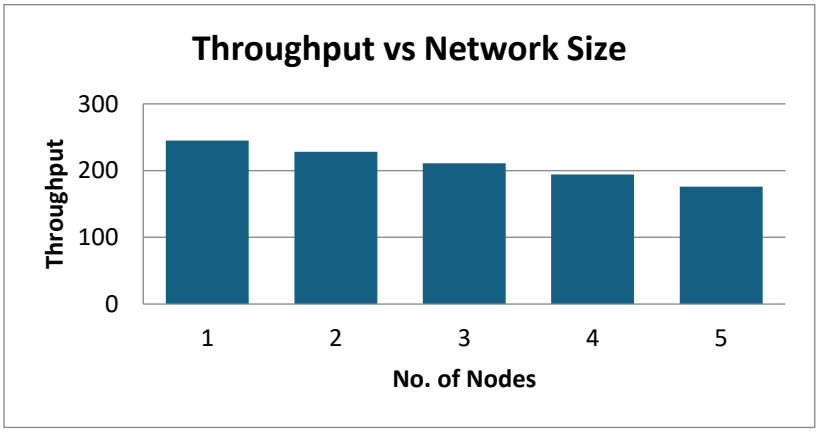

Fig. 3 Throughput vs Number of Nodes

Fig. 3 illustrates the variation of throughput with increasing network size. It can be observed that throughput gradually decreases from 245 kbps for 10 nodes to 176 kbps for 50 nodes. This reduction is primarily caused by increased network congestion; packet collisions, channel contention, and routing overhead as more devices participate in communication. Despite the decline in throughput, the proposed trust evaluation framework continues to effectively monitor network performance and accurately assess node trustworthiness. The results indicate that larger network deployments introduce communication challenges that directly impact data transmission efficiency and consequently influence trust computation.

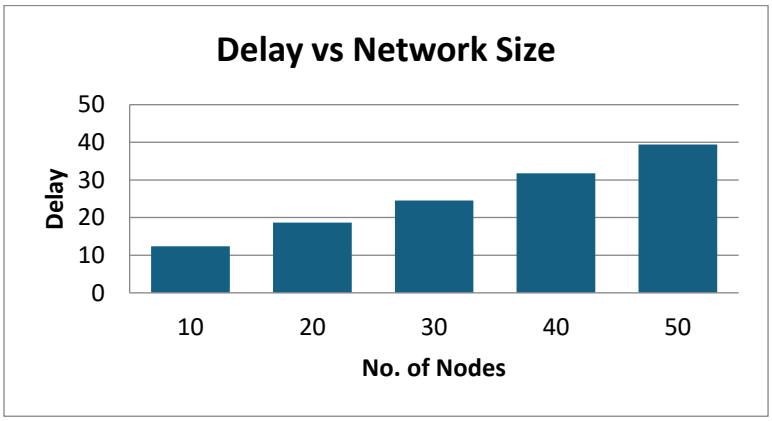

Fig. 4 Delay vs Number of Nodes

The increase in delay is primarily caused by higher network congestion, increased packet collisions, and additional routing overhead as more devices participate in communication shown figure 4. With a larger number of nodes, packets experience longer queuing times at intermediate nodes and require more processing before transmission. Consequently, the end-to-end delay gradually increases with network density. Despite this increase, the observed delay values remain within an acceptable range, demonstrating that the network can still maintain reliable communication under larger-scale deployments.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

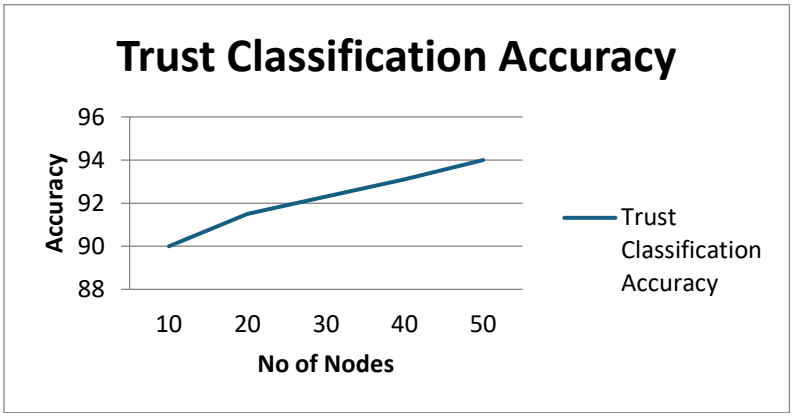

Fig. 5 Trust Classification Accuracy

The trust classification accuracy of the proposed entropy-based trust evaluation framework increases gradually as the network size grows from 10 to 50 nodes. As shown in figure 5, the accuracy improves from 90% for a 10-node network to 94% for a 50-node network. This improvement occurs because larger networks generate more communication observations and QoS data, allowing the entropy-based weighting mechanism to better distinguish between normal and abnormal device behavior. The results demonstrate that the proposed framework maintains high classification performance and scales effectively with increasing network size, making it suitable for large-scale IoT environments.

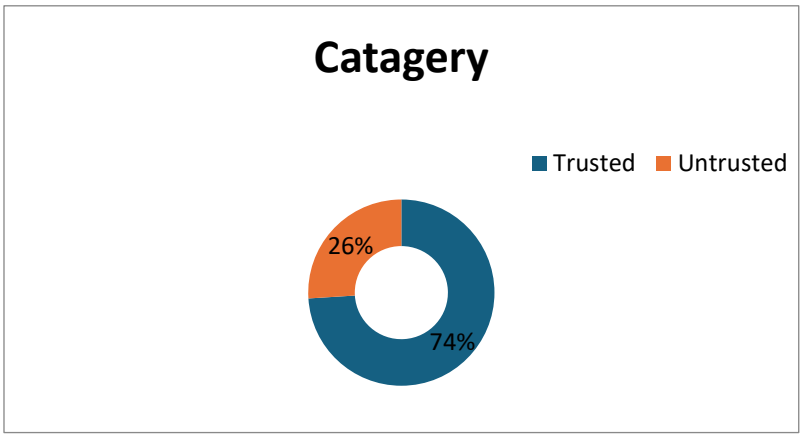

Fig.6 Trusted and Untrusted Nodes

Figure 6 illustrates the classification results obtained from the proposed entropy-based trust evaluation framework for a network consisting of 50 IoT devices. Based on the calculated trust scores and adaptive threshold mechanism, 37 nodes were classified as trusted, while 13 nodes were identified as untrusted.

Trusted nodes exhibited stable communication behavior characterized by high Packet Delivery Ratio (PDR), low end-to-end delay, and satisfactory throughput values. In contrast, untrusted nodes demonstrated degraded network performance, including increased packet loss, higher delays, and reduced throughput, resulting in trust scores below the established threshold. These results indicate that the proposed framework effectively differentiates reliable devices from potentially malicious or underperforming nodes, thereby improving the overall security and reliability of the IoT network.

The entropy weighting method dynamically determines the importance of each QoS metric based on the amount of information it contributes to trust evaluation. As shown in figure 7, Packet Delivery Ratio (PDR) receives the highest weight (37%), indicating that it has the greatest influence on distinguishing device behaviour. Throughput (32%) and Delay (31%) also contribute significantly to trust computation. The relatively balanced distribution of weights demonstrates that all three QoS parameters play an important role in evaluating device trustworthiness, while PDR remains the most discriminative metric for identifying trusted and untrusted nodes.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

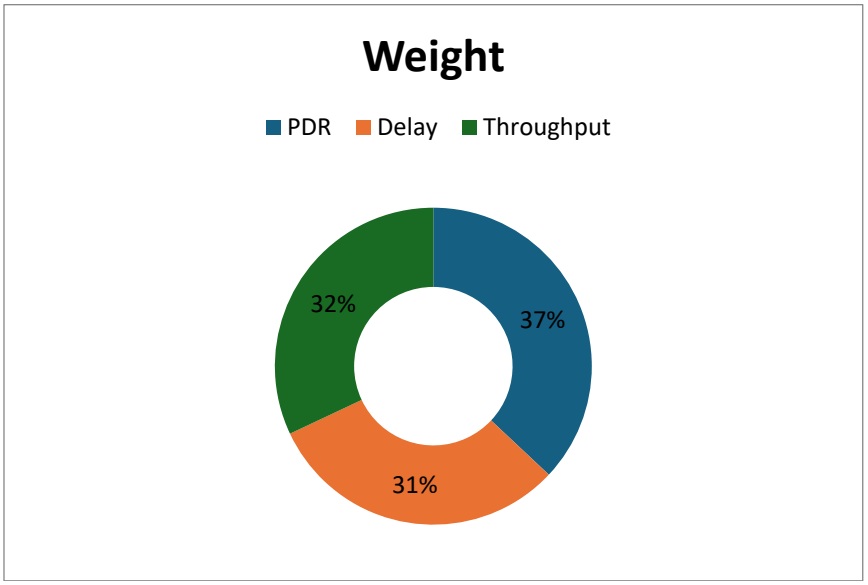

Fig.7 Entropy Weight Allocation

V. DISCUSSION

The experimental evaluation demonstrates the effectiveness of the proposed Entropy-Based Trust Evaluation Framework in identifying trusted and untrusted IoT devices using QoS metrics extracted from Contiki 3.0/Cooja simulation logs. Three key performance indicators, namely Packet Delivery Ratio (PDR), End-to-End Delay, and Throughput, were analyzed across different network sizes ranging from 10 to 50 nodes. The results indicate that increasing network density leads to a gradual decrease in PDR and throughput, while end-to-end delay increases due to higher contention, packet collisions, and routing overhead.

To accurately assess device behaviour, the extracted QoS metrics were normalized and processed using an entropy-based weighting mechanism. The entropy analysis assigned dynamic weights of 37%, 31%, and 32% to PDR, Delay, and Throughput, respectively, indicating that packet delivery reliability has the highest influence on trust estimation. Unlike conventional fixed-weight approaches, the proposed method automatically adapts metric importance according to their informational contribution, thereby improving trust discrimination capability.

The computed trust scores were evaluated using an adaptive threshold mechanism, enabling the classification of devices as trusted or untrusted. The results show that the framework consistently maintained high trust classification accuracy, ranging from 90% to 94% across all network scenarios. Furthermore, the trust distribution analysis successfully identified malicious or poorly performing nodes while preserving the reliability of well-behaved devices.
Overall, the findings validate that the proposed framework provides a lightweight, scalable, and adaptive trust management solution for heterogeneous IoT environments. By integrating QoS-based behavioural analysis with entropy-driven weighting and dynamic trust classification, the framework effectively enhances trust assessment accuracy and network reliability.

VI. CONCLUSION

The increasing deployment of heterogeneous Internet of Things (IoT) devices has intensified the need for efficient and adaptive trust management mechanisms capable of ensuring secure communication and reliable decision-making. Traditional trust evaluation approaches often rely on static weighting schemes, recommendation-based trust aggregation, or computationally intensive learning models, which may not adequately address the dynamic nature of IoT environments and evolving security threats.

This paper presented a Dynamic Trust Evaluation Framework (DTEF) that integrates Quality of Service (QoS)-based behavioural analysis with entropy-driven weighting and reputation-based trust updating. The proposed framework systematically evaluates device trustworthiness through five sequential stages: data collection, data processing, trust evaluation, trust validation, and trust updating. Network performance indicators, including Packet Delivery Ratio (PDR), end-to-end delay, and throughput, are extracted from IoT communication traces and normalized for trust

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2026

DOI: 10.17148/IARJSET.2026.13632

computation. An entropy-based weighting mechanism is employed to dynamically determine the significance of each trust attribute, enabling more accurate and adaptive trust estimation compared with conventional fixed-weight approaches.

Furthermore, the framework incorporates an adaptive threshold-based validation mechanism to classify devices as trusted or untrusted according to their behavioural characteristics. To maintain long-term reliability and resilience. This enables the framework to effectively respond to malicious activities, abnormal network behaviour, and changing operational conditions. The comparative analysis demonstrates that the proposed framework addresses several limitations of existing trust management approaches by combining lightweight computation, dynamic trust adaptation, and continuous reputation assessment within a unified architecture. As a result, the framework provides improved scalability, flexibility, and robustness for resource-constrained IoT environments.

Future work will focus on integrating Blockchain technology, for decentralized trust storage and verification, thereby enhancing transparency, immutability, and resistance against trust manipulation attacks. Additionally, advanced attack detection mechanisms targeting DDoS, Sybil, sinkhole, and on-off attacks will be incorporated to further strengthen trust management in large-scale IoT deployments.

REFERENCES

[1]. R. Chen, F. Bao, M. Chang, and J. Cho, “Trust management for secure communications in IoT,” IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1234–1245, 2018.

[2]. M. Nitti, L. Atzori, and I. P. Cvijikj, “Friendship selection in the Social Internet of Things,” *Computer Networks*, vol. 81, pp. 108–120, 2015.

[3]. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146–164, 2015.

[4]. Y. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Trust management system design for the Internet of Things,” *Computer Communications*, vol. 97, pp. 1–15, 2016.

[5]. V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K. R. Choo, “NeuroTrust: A Neuro-Fuzzy Trust Management Mechanism for Social Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5641–5651, 2020.

[6]. Alam, S.; Zardari, S.; Shamsi, J.A. Blockchain-Based Trust and Reputation Management in SIoT. *Electronics* 2022, *11*, 3871. https://doi.org/10.3390/electronics11233871

[7]. S. Faizullah, M. A. Khan, A. Alzahrani and I. Khan, "Permissioned Blockchain-Based Security for SDN in IoT Cloud Networks," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), Al Madinah Al Munawwarah, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/AECT47998.2020.9194181. keywords: {Access control;Switches;Internet of Things;Computer architecture},

[8]. F. Ullah et al., "Deep Trust: A Novel Framework for Dynamic Trust and Reputation Management in the Internet of Things (IoT)-Based Networks," in IEEE Access, vol. 12, pp. 87407-87419, 2024, doi: 10.1109/ACCESS.2024.3409273.