Improving the Security and Reliability of Cloud-Integrated WSNs with a Dynamic Trust Framework

Shalu[1,2]
[1]Post Doctoral Fellow
London Metropolitan University,
London, UK
[2]Manav Rachna University,
singshalu2609@gmail.com

Bal S.Virdee[3]
Professor
Director of the Centre for Communication Technology, London Metropolitan University, London, UK,
b.virdee@londonmet.ac.uk

Dr. Ashish Khanna[4]
Associate Professor
Maharaja Agrasen Institute of Technology,
New Delhi,
ashishkhanna@mait.ac.in

Abstract— **Wireless sensor networks (WSNs) coupled with cloud computing solutions are scalable, centralized storage, and processing with large scale monitoring applications. However, such integration intensifies security, trust, and resource-management issues due to limited resources of WSNs and distributed and multi-tenant characteristics of cloud platforms. In this study a dynamic trust framework has been proposed that is specific to cloud-integrated WSNs which combines direct and indirect trust, contextual behavior checking, reputation scoring with a fuzzy-logic trust fusion engine. The model relies on the concepts of data trust, communication reliability, energy trust, and behavioral anomalies to compute node trustworthiness, makes it possible to update trust periodically, and has a trust-sensitive isolation protocol. The model is deployed in CloudSim environment and evaluated under attack conditions and demonstrates superior malicious-node detection, high packet delivery rates, and prolonged network lifetime with the acceptable energy overheads. The findings show that the framework can be applied in the real-life cloud-WSN deployments.**

Keywords—Trust Model, Security, Reliability, Detection rate, Fuzzy logic, RFSN, GSTM.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are fundamental to modern monitoring systems in environmental monitoring, healthcare, smart cities, and industrial automation [1]. Their cost-efficiency, distributed sensing features allow ubiquitous data acquisition, and their resource limits (limited energy, computation, and memory) and wireless openness pose them to a variety of attacks: data falsification, node impersonation, selective forwarding, and Sybil attacks. Cloud integration can solve most of the WSN limitations, as it provides elastic storage, heavy computation of analytics, and centralized control [2]. It possesses inherent problems of trust and security; yet, additional complexities have emerged: multi-domain trust assessment, latency-sensitive decision-making, and the necessity to harmonise local trust (inside the network) with global policy (in the cloud). [3]

Trust management is a feasible method of measuring node reliability and leading to safe cooperation [4]. Reputation-based, behavior-based, and hybrid models are established frameworks of trust; nevertheless, they have made limited progress in addressing cloud-integrated wireless sensor networks due to insufficient emphasis on dynamic environments and cross-layer integration, as well as cloud-level aggregation and decision-making [5]. The paper presents a context-sensitive trust framework that (1) integrates both direct and indirect trust evidence, (2) is based on contextual monitored behavior, (3) integrates different measures of trust using fuzzy logic, and (4) is used together with cloud services to compute and enforce trust globally, (5) Simulation and testing in a long-term CloudSim process with attack conditions.

Section 2 relates to the work survey. The trust model proposed is described in section 3. Section 4 explains the simulation environment, measures of evaluation and performance analysis. The analysis and simulation results are presented in Section 5. Section 6 provides the conclusion and future directions.

II. LITERATURE SURVEY

This section provides a summary of authoritative literature on the issue of trust and security in WSNs and reputation systems, fuzzy trust fusion, and integration of cloud-WSN. The analysis acknowledges the advantages and disadvantages of previous methodologies and promotes for the suggested framework.

Proposes a Bayesian reputation framework where each sensor increases the trust of its neighbors through direct measurements using Beta distributions; which is lightweight, is appropriate to energy constrained WSNs, and it is meant to increase the data integrity of faulty or malicious measurements. The paper presents update regulations, trust limits in isolation, and appraisal in sensor contexts, and is thus a fundamental reference in local trust computation in the context of cloud aggregation. [6]

Proposes CONFIDANT a collaborative reputation and penalty framework among MANETs that identifies packet switching and selfishness, propagates alarms, isolates malevolent nodes. The paper studies detection and false positives as well as trade-offs. The mechanisms for distinguishing reputation sharing and penalisation are relevant for establishing cross-domain trust propagation between Wireless Sensor Networks and cloud services. [7]

Presents a global reputation aggregation method using eigenvector centrality to compute stable global trust scores and mitigate collusion and unfair feedback in large P2P systems. Although computationally heavier than local schemes, Eigen Trust's global aggregation principles inform cloud side reputation consolidation for WSNs that require network wide trust views. [8]

This study suggests service level management of SIoT with trust measures as QoS and social relations, and scale offloading to cloud computing resource; evaluates convergence and fluctuation trade-offs of adaptive trust parameters. The paper can be applied when developing cloud assisted trust modules which can analyze service providers and sensor as service offerings. [9]

This study provides an in-depth taxonomy and comparison of various trust computation techniques, metrics, and dynamics in mobile networks with the emphasis on evaluation

methodology and typical trade-offs (accuracy vs. overhead). The survey assists in placing design decisions on cloud integrated WSN trust frameworks and has assessments metrics of reliability and security.[10]

This research proposes the application of fuzzy inference algorithms to integrate diverse indicators (packet delivery, delay, residual energy) into a singular trust score, effectively managing the inherent obscurity and imprecision of data. The fusion of fuzzy methods is especially applicable in cases when cloud analytics need to synthesize inaccurate indicators of local trust of varying sensors. [11]

Behavioral profiling and ML based anomaly detection surveys and frameworks in WSNs indicate the use of statistical and learning techniques to identify compromised nodes and insider threats; numerous studies integrate anomaly scores and reputation to make strong decisions. These designs train dynamic trust models based on cloud resources to train models and restraint periodically without edge-based lightweight inference [12].

Researches blockchain and distributed ledgers as a method to store reputation records that cannot be modified and routing metadata that can be audited; advantages are that it is tamper resistant, and auditable, whereas drawbacks include storage costs, latency costs, and communication overhead costs. These suggestions are educative in the process of developing immutable audit trails against cloud integrated trust logs, particularly against high assurance applications. [13] Integration studies on Cloud WSN suggests hybrid designs in which the cloud does heavy trust analytic, long term reputation aggregation and cross domain correlation and sensors do lightweight trust updates; they address the latency, privacy, and new attack points created by cloud dependency. These are studies that are focused on the issue of operational and threat model of a dynamic cloud integrated trust framework.[14]

Energy conscious trust Works in energy aware trust have included residual energy in trust or routing choices to trade security with network lifetime and have suggested mechanisms to prevent attacks based on energy depletion whilst ensuring honest nodes participate. These models are critical in developing dynamic trust models in cloud integrated WSNs that must maintain the longevity of the nodes without violation of security policy. [15]

The comparative analysis of enhancing the security and reliability of cloud-integrated wireless sensor networks (WSNs) utilising a dynamic trust framework is shown in Table 1 below.

TABLE I COMPARATIVE ANALYSIS

Reference	**Applicability**	**Resource Overhead**	**Attack Coverage**	**Scalability and Maturity**
Ganeriwal et al. RFSN [6]	WSN; edge-centric reputation	Low; Bayesian updates per neighbor	Data integrity; misbehavior detection	Moderate; well-studied in WSN literature
Buchegger & Le Boudec CONFIDANT [7]	MANET; applicable to clustered WSNs	Medium; messaging for reputation propagation	Routing misbehavior; packet dropping; false reports	Moderate; validated in simulations and prototypes
Kamvar et al. EigenTrust [8]	P2P; cloud aggregation for WSNs	High; global eigenvector computation	Collusion; unfair feedback; Sybil (partially)	High for P2P; mature in file-sharing systems
Raya & Hubaux data-centric trust [9]	WSN; MANET routing	Medium; cryptographic and trust checks	Routing attacks; false data injection	Moderate; strong conceptual work with prototypes
Chen et al. SIoT trust [10]	SIoT; cloud-assisted IoT	Low at edge; High in cloud; offloads analytics	Malicious services; SLA violations	Emerging; cloud integration focus
Fuzzy trust models [11]	WSN; noisy IoT environments	Low–Medium; fuzzy inference cost tunable	Uncertain evidence; mixed attacks	Moderate; many prototype studies
Behavior based anomaly detection [12]	WSN; IoT; cloud for training	Medium–High; ML training in cloud, inference at edge	Insider compromise; novel attacks	Growing; depends on dataset availability
Blockchain enabled trust [13]	IoT; P2P; cloud-WSN audit	High; ledger storage and consensus cost	Tampering; reputation manipulation	Immature for WSNs; promising for audit trails
Cloud WSN integration studies [14]	Cloud-WSN hybrid systems	Low at edge; High in cloud; offload heavy tasks	Cross-domain attacks; large-scale correlation	Emerging; architectural proposals and pilots
Energy aware trust models [15]	WSN; energy constrained IoT	Low–Medium; simple energy weighting	Energy depletion attacks; availability threats	Moderate; practical for lifetime optimization

Reputation systems (RFSN, CONFIDANT) offer powerful schemes to aggregate peer feedback, however, frequently fail to scale to cloud-integrated topologies and tend to assume stable connectivity. Behavior based anomaly detectors can identify new attacks and are, however, computationally costly to sensor nodes. Fuzzy fusion methods are used to deal with heterogeneity of metrics and need tuning and rule design. There are only limited literature discussing real-time, context-aware trust updates to reconcile local (cluster-level) trust to cloud-level global policies, and energy-sensitive. It is this gap that drives a fuzzy-fusion trust framework that is hybrid and uses cloud-based resources to conduct worldwide assessment without incurring heavy-weight computations in-network.

III. PROPOSED TRUST MODEL

The proposed architecture has four logical layers and is depicted in figure 1.

1. **Sensor Nodes (SN):** Data-sensing devices, which are resource-constrained, and transmit the data to cluster heads. They check simple local trust (e.g. simple consistency checks).
2. **Cluster Heads (CH):** Local aggregators where sensor data is received, local trust measurements calculated and anomaly pre-emptively the first.
3. **Base Station (BS):** Network equipment transmitting summaries of trusted information and aggregated data to the cloud.
4. **Cloud Trust Module (CTM):** This is a cloud-based module that performs global trust evaluation, aggregation of

long-term reputation, policy, and cross-cluster correlation. Hierarchical architecture takes advantage of local

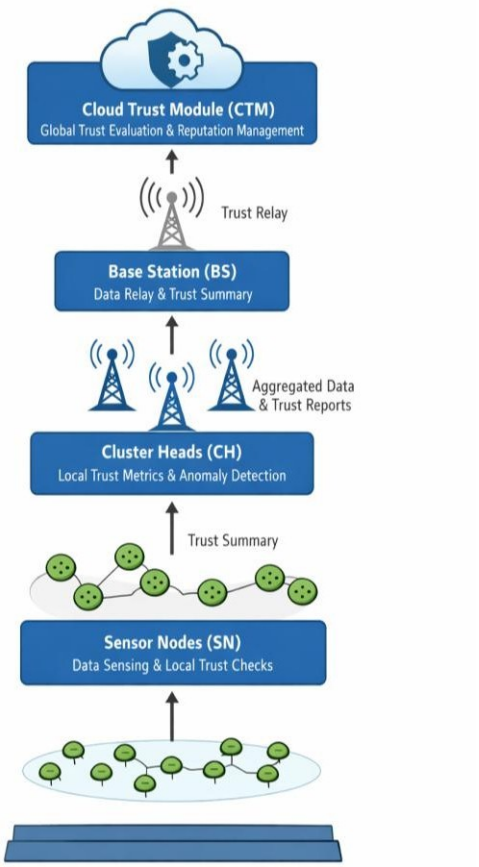

Fig 1. Proposed architecture

computing to minimize communication costs and store long-term reputation and analytics on cloud memory

A. Trust Metrics

In order to evaluate each node (i), the four supplementary metrics have been employed:

1) **Data Trust (DT):** Indicates the consistency of the sensed values of node (i) when compared to neighbors. DT between nodes (i) and (j):

$$DT(_{ij}) = 1 - \frac{|ki - kj|}{\max(ki - kj)}$$

Where ki and kj are sensed values.

2) **Communication Trust (CT):** Is a measure of success in delivering packets and link reliability.

$$CT(i) = \frac{P\ success}{PSuccess + Pfailure}$$

3) **Energy Trust (ET):** The normalized residual energy to prevent detection of nodes which are low on energy, but otherwise honest.

$$ET(i) = \frac{P\ success}{PSuccess + Pfailure}$$

4) **Behavior Trust (BT):** occurrence of abnormal and suspicious behavior (e.g. sudden shifts in patterns of reporting, unusual IDs).

$$BT(i) = 1 - \frac{anomalies}{total\_interactions}$$

B. Fuzzy Trust Fusion

Fuzzy Inference System (FIS) combines DT, CT, ET, and BT into one Final Trust Score (T(i)). The FIS operates on linguistic variables Low (0-0.3), Medium (0.3-0.7), High (0.7-1.0) of the inputs and a rule base that is more data and communication trust-driven and punishes the recurring abnormal actions. Example rules:

- when DT is High and CT is High and BT is High then Trust is High.
- When DT is Low, and BT is Low, Trust is Low.
- When ET is Low and DT is High THEN Trust is Medium (so as not to isolate low-energy honest nodes).
- To derive a numeric trust score in ([0,1]) the FIS output is defuzzified.

C. Trust Update Method

Trust is updated occasionally by a rule of exponential smooth:

$$T(i,m+1) = \beta \cdot T(i,m) + (1-\beta) \cdot Tlatest(i)$$

where $0 \leq \beta \leq 1$ controls inertia. An increase in β is more conducive to historical trust; a decrease results in an increase in trust responsiveness to recent behavior.

D. Evil Node Identification and Isolation

Thresholding: In case the value of T(i) is less than a threshold (T), the node (i) is marked as malicious.
Isolation: CHs discard packets of those nodes that are isolated and forward an isolation report to the BS and CTM.
Cloud Correlation: CTM also compares the isolation reports in clusters and detects the coordinated attacks, updating global reputations.

E. Indirect Trust and Reputation

The computation of indirect trust is based on the weighted recommendations of the neighbors based on their trustworthiness. The CTM adds long-term reputations and can nullify local choices in case there is cross-cluster proof of false positives.

F. Pseudocode: Trust Evaluation and Isolation

for each time epoch:
for each cluster_head CH:
for each node i in CH:
DT = calculate data credibility (i, neighbors)
CT = compute_comm_trust(i)
ET = compute_energy_trust(i)
BT = compute_behavior_trust(i)
T_new = fuzzy_fusion(DT, CT, ET, BT)
*T[i] = alpha * T[i] + (1 - alpha) * T_new*
if T[i] < threshold:

isolate_node(i)
report_to_cloud(i, T[i], DT, CT, ET, BT)
CTM gets reports and updates international reputations.
CTM can either command CHs to change thresholds or restore nodes.

IV. Simulation Setup

The simulation environment is expanded to include four new elements that model the roles of the different levels of architecture to support modelling of hierarchical trust of wireless sensor networks. The SensorNode element is the basic behavior of sensors devices such as data collection, simple local verification, and energy state monitoring. ClusterHead component will be local aggregators that combine the measurements of a subset of sensors, do minor

analytics, and calculate initial trust scores. The TrustManager component is the code that performs the calculation of metrics, the reinstatement of trust scores, and the local decision of reliability of nodes. Lastly, the CloudTrustModule component models the cloud side functionality, which includes long term reputation storage, worldwide trust assessment, and correlation between many the combination of these parts allows the simulator to replicate the lifecycle of trust events of a hierarchical system, local sensing and anomaly detection to the global aggregation and policy enforcement. A small fuzzy logic engine is also embedded in each cluster head to do real-time fusion of Data, Communication, Energy, and Behavior trust inputs, and the CTM is the host of a larger context, historical reputations, and policy rules to make global decisions. Behavior simulators inject attack scenarios, potentially at selective forwarding, falsified data, and Sybil attack rates and patterns, and therefore can be used to stress-test detection and mitigation mechanisms. The communication model explicitly models the behavior of packet loss, link reliability, and retransmission behavior in such a way that Communication Trust measures capture the behavior of real networks, and these link dynamics are used to input into local and global trust computations. Finally, an energy model keeps track of the cost of transmission and reception of per-packet and idle energy drain, updating the residual energy of each node and therefore the Energy Trust measure; these modules allow the simulator to trade off the detection accuracy, false positives, and network lifetime in a variety of adversarial and environmental conditions.

A. Evaluation Metrics

1) Detection Rate (DR): Proportion of true malicious nodes which are detected successfully.
2) False Positive Rate (FPR): The percentage of honest nodes falsely allocated.
3) Energy Overhead: Percentage change in the energy used in performing trust computations and reporting.
4) Packet Delivery Ratio (PDR): Packet deliveries that are successful to BS/cloud.
5) Network Lifetime: Time to first die and time to half die.

B. Performance Evaluation

The simulation is a cloud-based WSN with an extended version of CloudSim platform with 100 node network that is uniformly distributed on a 100 x 100 m area; the sensors begin with an initial energy of 2 J and cluster heads are constructed through an energy-sensitive clustering algorithm. The share of malicious nodes is set to 20 percent and operates on a set of adversary profiles that can be configured and the epoch length is a parameter that can be tuned, and the trust scores are updated at the termination of each epoch. Cluster leaders run to do local analytics, lightweight and send aggregated readings and summarized trust evidence to a base station which forwards the data to the cloud trust module that conducts long-term reputation aggregation and cross-cluster correlation. To test the framework, it is compared with two baseline frameworks: a reputation scheme which is based on the RFSN and a behavior-based anomaly detection scheme which is like the GTMS based on the following performance measures; detection accuracy, false positives, energy overhead, communication cost, and mitigation latency. The metric and their configuration are mentioned in Table 2 below:

TABLE III SIMULATION PARAMETER & THEIR DESCRIPTION

Simulation Parameter	Description
Simulator	Extended CloudSim 0
Network Specification	100 sensor nodes evenly spaced in a 100 m 100 m region
Initial Energy per Node	2 J
Cluster Formation	Cluster Heads (CHs) are picked with the help of an energy-sensitive clustering algorithm.
Malicious Nodes	20% of the nodes are selected as attackers randomly.
Epoch Duration	trainable; at the end of each epoch, the trust scores are updated.
Baseline Models for Comparison	RFSN-style reputation model. Behaviour-based model GTMS-like behaviour-based model.

V. RESULTS & ANALYSIS

In the following section, the three typical results of the simulation study are described (A) detection performance when the attack intensity is varied, (B) energy overhead as compared to a no trust baseline, and (C) comparisons of packet delivery ratio (PDR) and network lifetime. We provide the description of what is measured in each of these results, why the observed behavior is the consequence of the design decisions made in the trust framework, and how the baselines act differently, and what have practical implications on deployment and tuning.

A. Performance of detection at various malicious fraction

Detection Rate (DR) and False Positive Rate (FPR) rates were taken under different conditions of the ratio of the number of malicious nodes in the network. There are three operating points, 10, 20 and 30 percent malicious nodes. DR represents the rate of correctly identified and flagged malicious nodes, FPR is the rate of falsely flagged honest nodes.

Observed numbers.

- 10% malicious: DR $\approx$ 94%, FPR $\approx$ 4%.
- 20% malicious: DR $\approx$ 90%, FPR $\approx$ 6%.
- 30% malicious: DR $\approx$ 85%, FPR $\approx$ 8%.

It happens that the proposed hierarchical fuzzy trust model has high detection rates at lower and moderate adversary densities due to:

- Multi metric fusion (DT, CT, ET, BT) offers complementary evidence: inconsistencies in data and communication anomalies complement each other, and it is easier to detect single vector attacks.
- Local CH fusion swiftly denies misbehaviours that are easy to detect, whereas the CTM compares cross-cluster reports to identify coordinated attacks.

Numerous effects of high malicious fraction dilute DR and increase FPR:

1. Signal dilution: As the number of malicious nodes grows, the set of honest neighbours that one uses to compute pairwise Data Trust grows smaller, and it is more difficult to establish a stable baseline on which to compare. Neighbourhood statistics are easier to compromise with malicious nodes.

2. Collusion and recommendation attacks: The rogue nodes may join in collusion to provide false recommendations or to verify each other, and this will destroy indirect trust messages, unless there is heavy recommender weighting.

3. Resource contention and noise: The higher the adversaries use resources (selective forwarding, Sybil identities), the higher is the number of packets dropped and resent transmitted that can conceal both malicious and benign abnormalities that are hard to detect, increasing FPR.

The system has been designed with a narrow, false-positive design:

- Energy Trust (ET) regulates decisions such that low energy honest nodes are not isolated straight away.
- Fuzzy rules have the property that the various indicators (e.g. DT and CT both low) must be satisfied to say their trust is low, so they are not sensitive to the transient factors.
- Cloud correlation enables the CTM to confirm local isolation queries through cross cluster indications prior to global blacklisting and snare numerous false positive that are the result of localized environmental noise.

The findings indicate that the model is strong till moderate adversary densities (around 20 percent) with high DR and reasonable FPR. The detection is still useful in the higher densities (30%+), but more countermeasures are necessary (e.g., more recommenders, added sensors or adaptive thresholds) to achieve the same performance.

B. Energy overhead vs. baseline

It used the extra energy when performing trust calculations and infrequent reporting as comparisons to a no trust baseline (network operation without any trust-related processing or reporting).

Observed number. Trust functionality enhances energy consumption by approximately 20 percent about the no trust baseline.

Sources of overhead.

- Computation at CHs: The lightweight fuzzy inference engine can be used to perform computations which use CPU cycles and memory access which are converted to energy consumption.
- Periodic reporting: CHs and nodes periodically send the trust summaries and isolation reports to the BS/CTM; the additional transmissions and related acknowledgements are expensive in radio energy.

Factors contributing to moderate rather than substantial overhead.

- Lightweight on node processing: Sensor nodes do very little on-node checking, the more intensive fusion is done at CHs which is provisioned to be far more energy-consuming and processing-intensive.
- Energy conscious weighting and selective reporting: ET is a moderating input integrated in the fusion and the policy of the simulator has decreased the reporting frequency of low impact events. As an illustration, CHs consolidate several local anomalies in a single report as opposed to individual event messages.

Tradeoffs and tuning. The overhead of about 20 percent is a design point: it gives significant security and reliability gains (increased DR, improved PDR, increased lifetime) at a very affordable energy price. The operators can choose epoch length, reporting granularity, and smoothing parameter (alpha) to trade-off between energy and responsiveness: the longer the epochs, the bigger (alpha), the lower the overhead, but the lower the detection.

C. Packet Delivery Ratio and network lifetime comparison

Packet Delivery Ratio (PDR) on attack and network lifetime in terms of time to 50 node death were compared between the proposed model and two baselines (RFSN and GTMS).

Observed numbers.

- PDR: Proposed ≈ 92%, RFSN ≈ 85%, GTMS ≈ 88%. The proposed model has a complete PDR of approximately 92 percent in the attack, whereas RFSN and GTMS have 85 percent and 88 percent respectively.
- Network lifetime (50 percent nodes dead): Proposed saves lifetime by 15 percent compared to GTMS, GTMS compares to RFSN by only 2 percent; proposed model 15 percent compared to GTMS, unknown percentage compared to RFSN.

The performance of Proposed Trust Model in Comparison to RFSN and GTMS Frameworks is described in Table 3:

TABLE IIIII PERFORMANCE OF PROPOSED TRUST MODEL IN COMPARISON TO RFSN AND GTMS

Metric	**Proposed Model**	**RFSN**	**GTMS**
Detection Rate (20% malicious)	90%	88%	85%
False Positive Rate	6%	10%	8%
Energy Overhead	+20%	+18%	+15%
Packet Delivery Ratio	92%	85%	88%
Network Lifetime (50% nodes dead)	+15%	+5%	+2%

D. Analysis

The offered implementation balances detection effectiveness as well as resource expenditure thoroughly: the addition of a lightweight fuzzy fusion engine at cluster heads and using cloud-level correlation in the Cloud Trust Module enhance the detection effectiveness of both single-point and coordinated attacks, however, there exists a reasonable energy and processing cost that can be mitigated by design options such as the reduced size of the FIS at CHs and the adjustable inertia parameter. α that regulates the speed of trust responding to new information and thereby balances responsiveness and stability. To minimize the false positives, isolation decisions are not considered final and instead isolation reports and supporting evidence are submitted to the CTM to cross-cluster validate to allow anomalous but harmless events (such as environmental disturbances affecting many nodes) to be separated out and the CTM to revoke or revise local actions once it knows that the global context suggests false alarm. Energy efficiency is explicitly taken care of in the fusion process with the addition of Energy Trust (ET) as a moderating input node with low residual energy do not necessarily suffer penalties should their data and communication behaviour remain unchanged, thus ensuring that no unnecessary isolation of the honest but energy-depleted nodes occurs and enhancing the overall lifetime of the network.

Lastly the hierarchical processing model, which is computations of local metrics and CH-level fusion with cloud-level aggregation and long-term reputation management,

scales the system to large deployments, leaving the capability of executing the complex, global correlation and policy enforcement as required.

VI. Conclusion

The framework introduced in this study is a dynamic trust framework of cloud integrated wireless sensor networks that integrates data, communication, energy, and behavior metrics via a fuzzy logic engine into a hierarchical architecture where lightweight in network calculations is performed at cluster heads and cloud based global correlation and long-term reputation management is achieved at an acceptable energy cost. Simulation in an extended CloudSim environment indicates that the scheme can achieve high detection rates, low false positives, better packet delivery, and greater network lifetime at only an acceptable energy cost. The hierarchical architecture makes use of cluster level fuzzy fusion, such that per node processing and communication costs are kept low, and that compute intensive cross cluster correlation and policy enforcement is left to the Cloud Trust Module which not only authenticates local isolation decisions but also improves reputations over time. The framework will be tested later sensor testbeds and edge-cloud platforms to get an idea of how it works and how it can be implemented in the future. We will introduce a feature of adaptive learning that allows us to automatically set both the fuzzy rules and the trust inertia factor. Individual cam considers the possibility of storing reputation information in an irreversible fashion on blockchain or other tamper-evident ledgers and that cross-domain trust sharing can be realized. The privacy-preserving aggregation methods will be examined to calculate the scores of trusts without disclosing the sensitive sensor data. Lastly, we would like to expand the model to be able to support heterogeneous and mobile environment, i.e. supporting technologies like LoRaWAN, NB-IoT, and 5G, to ensure that the paradigm can be efficient and scaled to a wide group of real worlds IoT applications.

VII. Future Scope

The evaluation of the proposed trust framework will be conducted for real world deployments in future research which is beyond simulation-based verification that can deliver promising results. To investigate latency, energy efficiency, and detection accuracy in situations that are close to realistic wireless networking, experimental testbeds using low-power sensor platforms such as Raspberry Pi or Arduino will be setup. The communication overhead in heterogeneous environments and computational efficiency will also be analysed for networks with more than 500 nodes by performing scalability analysis. In a dynamic setup, latency evaluation will be performed by measuring the time it takes for the static trust updates to be completed, and in large scale IoT deployments, scalability experiments will be conducted. Altogether, these directions are meant to guide the framework towards an efficient and flexible industrial solution for smart-city applications.

References

[1] M. A. Khan, Shalu, Q. N. Naveed, A. Lasisi, S. Kaushik, and S. Kumar, "A Multi-Layered Assessment System for Trustworthiness Enhancement and Reliability for Industrial Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 137, pp. 1997–2036, Jul. 2024, doi: 10.1007/s11277-024-11391-x.

[2] H. Sadia, T. Rahman, A. Rahim, I. Khan, N. Ullah, and S. A. Algamdi, "Enhancing privacy preservation and integrity in IoT-enabled wireless sensor networks through novel advanced cryptographic techniques," *Sci. Rep.*, May 2026, doi: 10.1038/s41598-026-48128-8.

[3] K. Tripathi, Shalu, S. Kaushik, S. Vyas, M. A. Khan, and A. Ahmadian, "TITAN: Logarithm-based trust-aware integrated technique for robust anomaly neutralization in industrial WSNs," *Peer--Peer Netw. Appl.*, vol. 19, no. 3, p. 79, Apr. 2026, doi: 10.1007/s12083-026-02222-w.

[4] E. D. L. Cruz, C. Prakash, and S. Rana, "AI-Driven Anomaly Detection and Zero Trust Frameworks: Securing Industrial IoT in Hybrid Cloud Ecosystems," in *Cybersecurity for Industrial IoT in Hybrid Cloud Environments*, IGI Global Scientific Publishing, 2026, pp. 297–350. doi: 10.4018/979-8-3373-4581-9.ch009.

[5] M. L N, S. M R, and A. N, "A Survey on Enhancing Information Security in Cloud-Enabled IoT Monitoring Systems," in *2026 4th International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, Apr. 2026, pp. 1–6. doi: 10.1109/ICKECS70176.2026.11527579.

[6] S. Ganeriwal, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sens. Netw. TOSN*, vol. 4, no. 3, p. 15:1-15:37, doi: 10.1145/1362542.1362546.

[7] Sonja Buchegger, "Performance analysis of the CONFIDANT protocol," pp. 226–236, Jun. 2002, doi: doi/10.1145/513800.513828.

[8] Sepandar D. Kamvar, Mario T. Schlosser, "The Eigentrust algorithm for reputation management in P2P networks," pp. 640–651, 2003, doi: https://doi.org/10.1145/775152.775242.

[9] L. Wei and Y. Qing, "A trust-based secure routing algorithm for wireless sensor networks," presented at the 34th Chinese Control Conference (CCC), Jul. 2015, pp. 7726–7729. doi: 10.1109/ChiCC.2015.7260866.

[10] I.-R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov. 2016, doi: 10.1109/TDSC.2015.2420552.

[11] T. K. Kim and H. S. Seo, "A Trust Model using Fuzzy Logic in Wireless Sensor Network," *Int. J. Electron. Commun. Eng.*, vol. 2, no. 6, pp. 1051–1054, Jun. 2008, doi: doi.org/10.5281/zenodo.1079192.

[12] A. Haque, M. N.-U.-R. Chowdhury, and I. Ahmed, "Wireless Sensor Networks anomaly detection using Machine Learning: A Survey," Jan. 2024, pp. 491–506. doi: 10.48550/arXiv.2303.08823.

[13] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J.-G. Choi, "Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks," *Sensors*, vol. 22, no. 2, p. 411, Jan. 2022, doi: 10.3390/s22020411.

[14] Buddesab, S. P. Bhavyashree, and J. Thriveni, "Integration of Wireless Sensor Network and Cloud Computing Using Trust and Reputation Technique," in *Emerging Research in Electronics, Computer Science and Technology*, Singapore: Springer, 2019, pp. 69–82. doi: 10.1007/978-981-13-5802-9_7.

[15] M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya & H. Abdul Gaffar, "Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks," no. 15, Jun. 2025, doi: https://doi.org/10.1038/s41598-025-03558-8.