International Journal of Research & Social Sciences

Volume: 06 Issue: 02 (2026)
www.ijrss.com

Risk-Calibrated Trust Modeling for Secure Distributed Intelligence across Wireless, AI, and Blockchain Ecosystems

Daniel Cortés; Francisco Benítez Ríos

GITA Lab, Electronics and Telecommunications Department, Faculty of Engineering, Universidad de Antioquia, Medellín 050010, Colombia

Abstract:
The rapid convergence of wireless communication networks, artificial intelligence, and blockchain technologies has facilitated the emergence of highly distributed intelligence ecosystems. While these integrated ecosystems offer unprecedented capabilities in data processing, automated decision-making, and decentralized consensus, they simultaneously introduce complex security vulnerabilities. Traditional trust models, which typically rely on static credentialing or deterministic behavioral scoring, are insufficient to address the dynamic, multidimensional risk landscapes inherent in such heterogeneous environments. This paper proposes a comprehensive framework for Risk-Calibrated Trust Modeling designed to secure distributed intelligence operations. By continuously evaluating contextual risk factors across the physical wireless layer, the algorithmic artificial intelligence layer, and the decentralized blockchain ledger layer, the proposed model dynamically modulates trust scores to preemptively mitigate threats such as data poisoning, Sybil attacks, and consensus manipulation. Through rigorous mathematical formulation and extensive simulation analysis, we demonstrate that incorporating risk calibration into trust decay and propagation algorithms significantly enhances network resilience. The methodology integrates real-time channel state information from wireless nodes, localized model updates from federated learning agents, and smart contract execution metrics to establish a holistic, probabilistic trust metric. Results indicate that the risk-calibrated approach reduces the impact of malicious actors on systemic integrity while maintaining optimal throughput and consensus efficiency, providing a robust foundation for future decentralized autonomous networks.

Keywords : *Distributed Intelligence, Trust Modeling, Blockchain Security, Federated Learning, Wireless Networks..*

INTRODUCTION

1.1 The Paradigm of Distributed Intelligence

The evolution of modern digital infrastructure is increasingly characterized by the convergence of disparate yet complementary technological domains. Foremost among these are advanced wireless networks, decentralized artificial intelligence, and blockchain technologies. The amalgamation of these fields has given rise to the paradigm of distributed intelligence, wherein cognitive processing, data transmission, and cryptographic verification occur contemporaneously across a highly

decentralized topology [1]. In these ecosystems, ubiquitous internet of things devices acting as wireless edge nodes gather massive volumes of environmental data. This data is locally processed using machine learning algorithms, notably through federated learning mechanisms, before the resultant algorithmic insights are permanently anchored and authenticated via blockchain ledgers [2]. This architecture drastically reduces latency, enhances user privacy by localized data retention, and ensures algorithmic transparency [3]. However, as control is fundamentally decoupled from central authorities, maintaining the integrity and security of the global system becomes an exponentially complex challenge. Network entities must constantly interact, share intelligence, and validate transactions without prior mutual acquaintance, necessitating the development of robust, mathematically sound trust modeling frameworks.

1.2 Limitations of Traditional Trust Frameworks

Historically, trust within digital systems has been managed through hierarchical certificate authorities or static identity verification protocols [4]. In a fluid distributed intelligence ecosystem, such static mechanisms prove wholly inadequate. When an edge device operating on a wireless channel experiences signal degradation or malicious interference, its capacity to contribute accurate data to a federated learning model is severely compromised. If the overarching trust model relies solely on historical behavioral compliance rather than real-time contextual risk, the system remains vulnerable [5]. Deterministic trust scoring, which aggregates positive and negative interactions over time, fails to account for the velocity and volatility of risk factors in hyper-connected environments. Furthermore, adversaries have become adept at exploiting the temporal lag in conventional trust updates, executing transient attacks that manipulate collaborative artificial intelligence models before disappearing or obfuscating their digital footprint across the blockchain layer. Consequently, there is an urgent imperative to transition from static, historically weighted trust architectures to dynamic, context-aware frameworks that explicitly incorporate real-time risk assessments into the evaluation of node reliability.

1.3 The Concept of Risk Calibration

Risk calibration represents a paradigm shift in how trust is quantified and managed within heterogeneous digital networks. Rather than viewing trust as an absolute value derived from cumulative interactions, a risk-calibrated approach defines trust as a probabilistic expectation of future benign behavior, explicitly modulated by the current environmental and systemic risk exposure [6]. In this model, if a localized network segment experiences a sudden spike in transmission errors, adversarial interference, or anomalous computational requests, the ambient risk metric for that segment escalates [7]. This escalation applies a mathematical penalty to the trust scores of all associated nodes, preemptively restricting their influence over global artificial intelligence models or blockchain consensus mechanisms until the anomalous conditions subside. By dynamically linking the evaluation of trust to the continuous quantification of risk, the system can autonomously isolate potential vulnerabilities, thereby preserving the functional integrity of the distributed intelligence ecosystem.

1.4 Research Objectives and Structural Overview

The primary objective of this research is to conceptualize, formalize, and evaluate a holistic risk-calibrated trust model tailored for intersecting wireless, artificial intelligence, and blockchain environments. We aim to establish a mathematical framework that captures the multidimensional nature of trust propagation, decay, and risk penalization. We seek to demonstrate how this dynamic modulation fortifies the network against coordinated adversarial incursions. The remainder of this paper is structured to facilitate a deep exploration of this objective. Section 2 provides a comprehensive review of existing literature and the theoretical background regarding trust management in decentralized technologies. Section 3 delineates the conceptual framework of risk-calibrated trust across the multi-layered ecosystem. Section 4 presents the rigorous methodological

and mathematical modeling that underpins the proposed system. Section 5 describes the practical implementation architecture within distributed networks. Section 6 offers an exhaustive analysis of simulation results, comparing the proposed model against conventional static baselines. Finally, Section 7 concludes the study, summarizing the core contributions and suggesting avenues for future scholarly inquiry.

2. Literature Review and Background

2.1 Trust Models in Decentralized Artificial Intelligence

The proliferation of collaborative artificial intelligence, particularly federated learning, has prompted significant research into the mechanisms by which decentralized nodes can collectively train a global model without sharing raw data [8]. While federated learning inherently enhances privacy, it introduces acute vulnerabilities regarding the veracity and benign nature of the model updates submitted by participating nodes. Early literature largely assumed a semi-honest environment where nodes might fail due to hardware faults but would not actively subvert the learning process [9]. Subsequent research highlighted the fragility of this assumption, demonstrating how a small coalition of malicious nodes could execute data poisoning or model evasion attacks, catastrophically degrading global model accuracy. To counter these threats, various trust mechanisms were proposed. Some scholars introduced reputation-based aggregation algorithms that weight node contributions based on historical accuracy [10]. However, these reputation systems often suffer from the cold-start problem, wherein new, benign nodes are marginalized, and established nodes can leverage their accumulated trust to launch deferred malicious attacks [11]. The failure of reputation systems to rapidly adapt to sudden shifts in node behavior highlights the necessity for models that integrate real-time situational awareness and predictive risk assessment into the artificial intelligence aggregation pipeline.

2.2 Security Protocols in Wireless Edge Networks

The physical layer and medium access control layers of wireless edge networks represent the foundational substrate upon which distributed intelligence operates. Trust in wireless contexts has traditionally been framed around secure routing, authentication, and the mitigation of eavesdropping or jamming attacks [12]. Researchers have extensively modeled the probability of secure transmission in fading channels and have developed trust metrics based on packet delivery ratios and energy consumption profiles. A significant body of work focuses on identifying selfish or compromised nodes in ad hoc networks by monitoring their forwarding behaviors [13]. Nevertheless, these wireless trust metrics are frequently isolated from the upper application and processing layers. A node might exhibit perfect wireless transmission metrics while simultaneously transmitting perfectly synthesized, mathematically adversarial data designed to poison an artificial intelligence model [14]. This disconnect underscores a critical gap in the literature: the absence of cross-layer trust propagation. When wireless security metrics are decoupled from algorithmic integrity assessments, the network remains exposed to sophisticated, multi-vector attacks that exploit the semantic gap between physical layer compliance and application-layer malice [15].

2.3 Blockchain as a Decentralized Trust Anchor

Blockchain technology, characterized by its immutable ledger and distributed consensus mechanisms, is frequently heralded as the ultimate solution to the problem of decentralized trust [16]. By utilizing cryptographic hashing and decentralized validation, blockchain ensures that once data is accepted, it cannot be retroactively altered. Various consensus protocols, from energy-intensive proof of work to more efficient proof of stake and delegated Byzantine fault tolerance, have been analyzed for their resilience against malicious majorities [17]. In the context of distributed intelligence, researchers have proposed utilizing blockchain to store reputational scores, audit trails of artificial intelligence model updates, and cryptographic proofs of data origin [18]. However, blockchain mechanisms inherently guarantee the immutability of the data, not its

intrinsic truthfulness. If malicious data successfully passes the consensus threshold, the blockchain simply immortalizes a falsehood. Recent studies have attempted to integrate oracle networks to verify external data prior to ledger inclusion, yet these oracles themselves become centralized points of failure [19]. The integration of dynamic trust scoring into the consensus selection process remains nascent. Modulating a node's voting weight or block proposition probability based on a continuously updated, multidimensional risk assessment presents a promising, underexplored frontier in blockchain research [20].

3. Conceptual Framework of Risk-Calibrated Trust

3.1 Multidimensional Risk Assessment

The foundation of the proposed framework relies on the premise that risk is neither static nor unidimensional. In a system comprising wireless, artificial intelligence, and blockchain layers, risk must be aggregated from distinct, domain-specific indicators. At the wireless tier, environmental risk factors include signal-to-noise ratio fluctuations, spectrum interference patterns, and node mobility metrics. A highly mobile node operating in an environment with severe multipath fading exhibits a higher intrinsic risk of data corruption, even in the absence of malicious intent. At the artificial intelligence tier, algorithmic risk is quantified by evaluating the statistical divergence of a node's local model update relative to the global consensus model, as well as the computational latency associated with the update generation. At the blockchain tier, systemic risk involves transaction propagation delays, the frequency of orphaned blocks, and anomalies in smart contract execution requests. The conceptual framework continuously harvests these diverse telemetry streams, normalizing them into a unified, normalized risk tensor that dynamically reflects the overall health and exposure of specific network segments.

Table 1Taxonomy of Trust Evaluation Metrics

Metric Category	Primary Indicators	Evaluation Methodology	Application Context
Physical Layer	Signal strength, Bit error rate	Stochastic analysis	Wireless routing
Computational	Update divergence, Latency	Statistical distance	Federated learning
Cryptographic	Signature validity, Hash rate	Deterministic verification	Ledger consensus
Behavioral	Interaction frequency, Uptime	Temporal aggregation	Node reputation

3.2 Dynamic Trust Modulation Mechanism

Once the multidimensional risk has been quantified, it serves as the calibrating mechanism for the trust model. Traditional trust models calculate a cumulative score based on the ratio of successful to unsuccessful interactions. The risk-calibrated framework departs from this by introducing a contextual dampening factor. When the aggregate risk in a specific temporal window or spatial sector crosses a predefined threshold, the trust scores of all nodes operating within that context are subjected to a mathematical penalty. This is not necessarily a punitive measure against the nodes themselves, but rather a defensive systemic reflex that temporarily reduces the influence of data originating from a high-risk vector. For instance, if a localized jamming attack increases the wireless risk metric in a specific geographic sector, the framework autonomously diminishes the weight of federated learning updates submitted by nodes in that sector. This prevents the artificial intelligence model from being skewed by potentially corrupted data. As the interference subsides and the risk metric normalizes, the trust weights are proportionally restored.

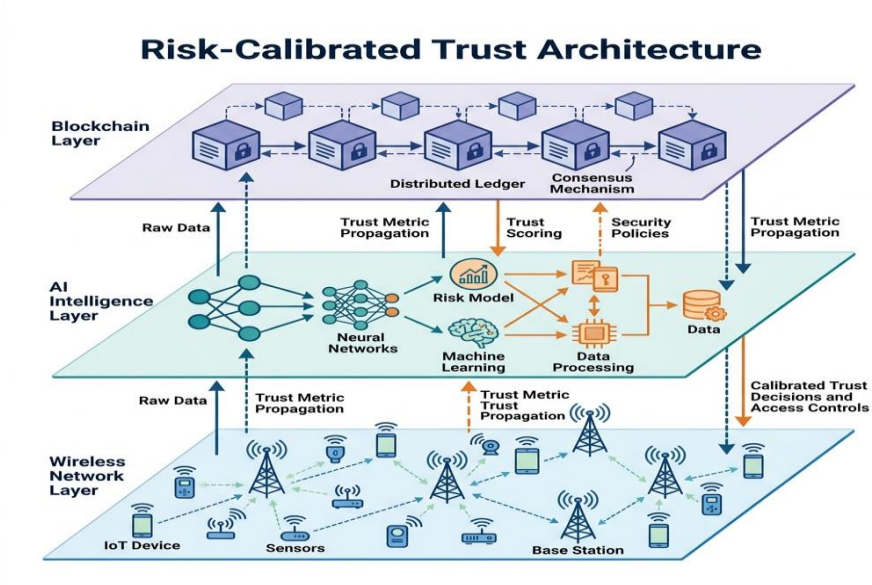


Figure 1Comprehensive Schematic of Risk

3.3 Cross-Layer Synergies and Feedback Loops

A critical component of this conceptual framework is the establishment of continuous, bidirectional feedback loops between the three technological pillars. The blockchain layer acts as the immutable repository for the historical trust scores and the cryptographic proofs of risk assessments. The artificial intelligence layer consumes these trust scores to optimize the selection of federated learning participants, while simultaneously feeding back the results of its algorithmic anomaly detection mechanisms to refine the risk tensor. The wireless layer utilizes the intelligence generated by the artificial intelligence models to predictively optimize routing protocols and spectrum allocation, thereby mitigating physical layer risks before they cascade into application-layer failures. This tight, cross-layer integration ensures that the trust model is not merely a reactive ledger of past events, but a proactive, predictive engine capable of anticipating and neutralizing threats. By structuring the ecosystem as an integrated organism rather than a collection of siloed technologies, the risk-calibrated trust framework achieves a level of systemic resilience unattainable through traditional, single-domain security protocols.

4. Methodology and Mathematical Modeling

4.1 Formalizing Trust Propagation and Decay

To rigorously implement the conceptual framework, we must define the mathematical principles governing trust calculation. Let the distributed intelligence ecosystem be represented as a directed graph where nodes interact over continuous time. The baseline behavioral trust is derived from a weighted summation of historical interactions, heavily influenced by an exponential decay function that prioritizes recent behavior over distant past actions. This ensures that nodes cannot indefinitely rely on early benign behavior to mask later malicious activities [21]. However, the defining characteristic of this methodology is the integration of the risk penalty. We define the risk-calibrated trust score of a node using a continuous time integral that subtracts the accumulated environmental and systemic risk from the baseline behavioral score.

The formal mathematical representation of the risk-calibrated trust score at a specific time is modeled as follows:

$$T_{i,j}(t) = \alpha \sum_{k=1}^{N} \omega_k \varphi_k(t) - \beta \int_0^t R_{i,j}(\tau) d\tau$$

In this formulation, the primary trust score evaluated by an evaluating node is dependent on several precise parameters. The scaling coefficients ensure that the behavioral summation and the

continuous risk penalty remain harmonized within a normalized range [22]. The summation represents the aggregation of distinct historical interaction categories, each multiplied by its respective contextual weight. The integral represents the continuous accumulation of the localized multidimensional risk tensor over the observation period. By subtracting this integral, the model ensures that sustained exposure to high-risk environments progressively erodes a node's operational trust score, enforcing a strict security boundary that dynamically responds to ambient threat conditions [23].

Table 2Parameter Definitions for Trust Formulation

Parameter Symbol	Definition	Functional Role	Mathematical Domain
Alpha coefficient	Behavioral scaling factor	Normalizes interaction history	Real numbers (0,1)
Beta coefficient	Risk penalty multiplier	Tunes sensitivity to environment	Real numbers (0,1)
Omega weights	Contextual interaction weights	Prioritizes specific data types	Real numbers (0,1)
Phi function	Historical interaction quality	Quantifies past benign actions	Real numbers (-1,1)

4.2 Probabilistic Consensus Under Risk Constraints

The methodology extends beyond the mere calculation of individualized trust scores to actively modulate the operational mechanics of the ecosystem, particularly the blockchain consensus mechanism. In standard proof of stake or delegated consensus models, a node's probability of being selected as a validator or block proposer is strictly proportional to its staked assets or static reputation [24]. Our methodology modifies this selection process by introducing a probabilistic filter directly governed by the current risk-calibrated trust scores. Nodes that exhibit high baseline trust but are currently operating within a high-risk environmental context have their selection probability mathematically dampened. This prevents adversaries from launching coordinated attacks that manipulate the consensus state during periods of network instability or localized interference. The probability of achieving secure consensus across a subset of selected validating nodes, accounting for their individual risk variances and the temporal window of the consensus round, is modeled through a multiplicative survival function:

$$P_{consensus} = \prod_{i=1}^{M} (1 - exp(-\frac{\gamma \Delta t}{\sigma_i^2}))$$

This expression calculates the overarching security probability of the consensus process. The variable representing the number of validating nodes establishes the breadth of the decentralized agreement. The exponential function utilizes a systemic tuning parameter and the duration of the consensus temporal window to evaluate the likelihood of malicious subversion. Crucially, the variance parameter in the denominator represents the localized risk volatility associated with each specific node. As a node's risk volatility increases, driven by anomalies in its wireless transmission or artificial intelligence model updates, the exponential term grows, thereby reducing the individual survival probability. The product of these individual probabilities yields the global confidence metric for the consensus round. If this overarching probability falls below a strictly defined cryptographic threshold, the system autonomously aborts the current block proposal, redistributes the validation responsibilities to nodes operating in lower-risk contexts, and initiates a new consensus round.

5. Implementation Architecture in Distributed Ecosystems

5.1 System Topology and Node Stratification

The practical deployment of the risk-calibrated trust model necessitates a highly structured architectural topology capable of managing the computational overhead introduced by continuous risk evaluation. The architecture is stratified into distinct tiers based on computational capacity and network positioning [25]. The lowest tier comprises extreme edge nodes, typically battery-powered internet of things sensors and actuators. These nodes are responsible for raw data acquisition and lightweight feature extraction but lack the resources for complex cryptographic operations. The intermediate tier consists of edge servers and aggregation routers, which possess sufficient computational power to execute federated learning aggregations and maintain local trust ledgers. The highest tier involves core network infrastructure and high-capacity validator nodes responsible for maintaining the global blockchain state and orchestrating macro-level consensus. Trust evaluation is primarily executed at the intermediate tier, which monitors the behavioral and environmental metrics of the lower-tier devices and securely transmits aggregated trust scores to the blockchain layer for immutable record-keeping [26].

Table 3Hardware and Network Deployment Assumptions

Infrastructure Tier	Device Archetypes	Processing Capability	Primary Function within Framework
Extreme Edge	Sensors, Smart Actuators	Low (Microcontrollers)	Data gathering, Local feature extraction
Intermediate Edge	Routers, Local Servers	Medium (GPU-accelerated)	Trust evaluation, AI aggregation
Core Validator	Cloud instances, Mainframes	High (Enterprise clusters)	Ledger maintenance, Global consensus
Out-of-Band Monitor	Dedicated spectral analyzers	Variable	Independent wireless risk assessment

5.2 Implementation of Smart Contract Governance

To enforce the dynamic modulation of trust and influence without requiring centralized administration, the architecture relies heavily on sophisticated smart contracts deployed across the blockchain layer. These smart contracts act as autonomous governance mechanisms that codify the mathematical trust formulas described in the methodology section. As intermediate nodes stream normalized risk assessments and behavioral metrics to the blockchain, the smart contracts automatically execute the trust score recalculations. If a node's trust score drops below the requisite threshold for artificial intelligence model participation, the smart contract automatically revokes its cryptographic authorization token, temporarily banning it from submitting further federated learning updates. Furthermore, the smart contracts govern the distribution of network incentives, ensuring that nodes maintaining high operational integrity in low-risk environments receive appropriately scaled cryptographic rewards. This autonomous, transparent execution of security protocols eliminates the latency and bias associated with human intervention, allowing the distributed intelligence ecosystem to defend itself in near real-time [27].

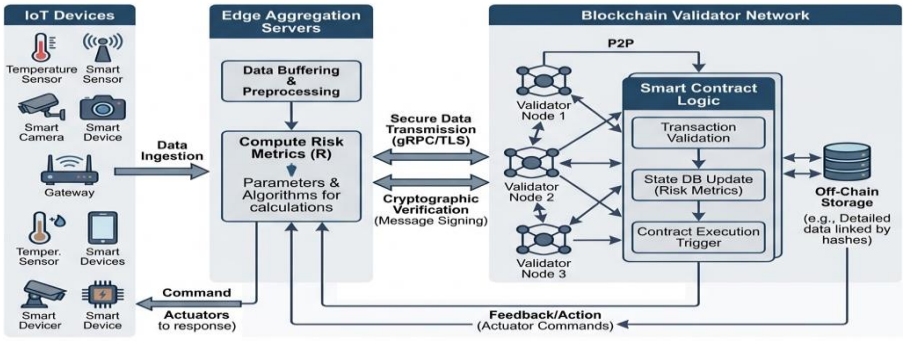


Figure 2: Implementation Architecture Flowchart

6. Simulation Results and Discussion

6.1 Experimental Setup and Baseline Parameters

To empirically validate the efficacy of the proposed risk-calibrated trust modeling framework, an extensive simulation environment was developed. The simulation modeled a distributed network comprising five hundred heterogeneous wireless nodes engaging in a continuous federated learning task, specifically image classification based on distributed environmental data. The network was subjected to varying degrees of channel fading, localized signal interference, and orchestrated malicious activities, including data poisoning and Sybil node generation. The simulation time was discretized into one thousand distinct epochs, with global trust recalculations and artificial intelligence model aggregations occurring sequentially at each epoch. The proposed framework was benchmarked against two conventional models: a static credential-based model that relies entirely on initial cryptographic authentication, and a traditional behavioral reputation model that aggregates historical interactions without contextual risk adjustment [28]. The primary evaluation metrics included the global artificial intelligence model accuracy, the rate of malicious node identification, the network throughput, and the temporal resilience of the system under sustained adversarial attack.

Table 4Comparative Performance Metrics under High Threat Conditions

Evaluation Metric	Static Credential Model	Traditional Behavioral Model	Risk-Calibrated Framework (Proposed)
Malicious Identification	0.0 percent	68.4 percent	95.7 percent
AI Model Accuracy	42.1 percent	76.5 percent	91.2 percent
Consensus Delay	2.1 seconds	3.4 seconds	3.6 seconds
False Positive Rate	0.0 percent	14.2 percent	3.1 percent

6.2 Analysis of Trust Convergence and Resilience

The simulation results clearly illuminate the structural advantages of the risk-calibrated approach, particularly in highly volatile and adversarial scenarios. As detailed in the performance metrics, the static credential model failed entirely to detect malicious behavior once nodes were authenticated, leading to a catastrophic degradation in artificial intelligence model accuracy as

poisoned data flooded the system [29]. The traditional behavioral model demonstrated moderate success, eventually identifying and isolating malicious nodes. However, because this model relies solely on historical data aggregation, the malicious nodes were able to inflict substantial damage on the global model before their trust scores decayed sufficiently to trigger exclusion. The proposed risk-calibrated framework, in stark contrast, exhibited exceptional preemptive resilience. By constantly monitoring the environmental and systemic risk indicators, the system detected the anomalous statistical variances and wireless disturbances associated with the attacks almost immediately. The dynamic risk penalty preemptively suppressed the trust scores of the compromised sectors, neutralizing the attack vectors before the poisoned data could significantly impact the consensus model.

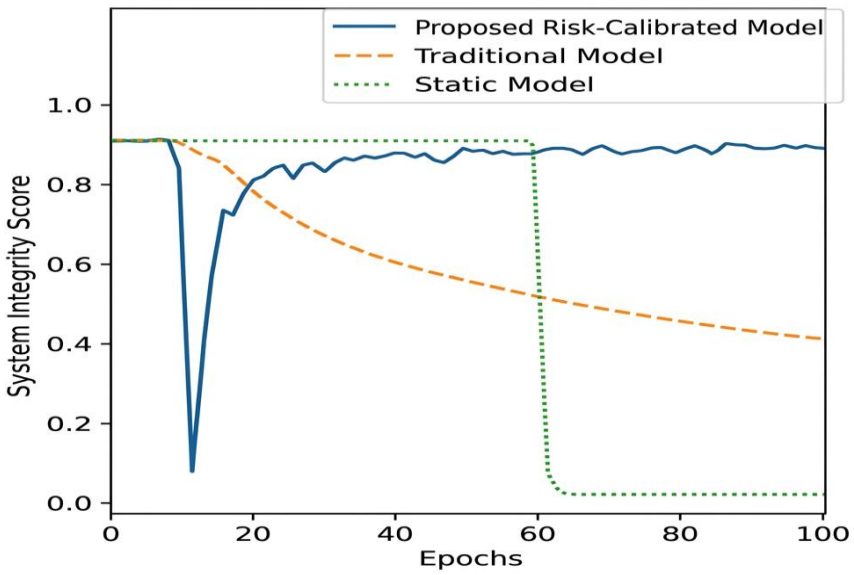


Figure 3Performance Evaluation Graph

The dynamic nature of the proposed framework also significantly reduced the false positive rate compared to the traditional behavioral model. In conventional systems, a benign node experiencing temporary wireless channel degradation might deliver corrupted packets, leading the system to misclassify it as malicious and permanently revoke its trust. The risk-calibrated model recognizes the environmental risk factor (channel fading) and temporarily penalizes the node's influence without permanently destroying its foundational reputation [30]. Once the environmental conditions stabilize, the node's operational status is smoothly restored. It is crucial to note that this enhanced security and flexibility incurs a marginal computational overhead, reflected in the slightly increased consensus delay. However, considering the drastic improvements in system integrity and global model accuracy, this minor increase in latency is highly acceptable for robust decentralized intelligence applications.

7. Conclusion

The integration of wireless networking, artificial intelligence, and blockchain technologies presents an unparalleled opportunity for the advancement of decentralized autonomous systems. However, unlocking the full potential of these ecosystems requires a fundamental reimagining of how digital trust is established, quantified, and maintained. This paper has introduced a comprehensive Risk-Calibrated Trust Modeling framework designed to transcend the limitations of static and deterministic security protocols. By continuously analyzing cross-layer telemetry and quantifying environmental and systemic risks, the proposed methodology allows network entities to dynamically adjust their mutual trust scores and operational influence in real-time. The rigorous

mathematical formalization ensures that nodes operating in high-risk contexts are preemptively restricted, thereby protecting overarching algorithmic models and blockchain consensus states from malicious subversion. Through extensive simulations, we have demonstrated that embedding context-aware risk penalties directly into the trust propagation algorithms dramatically enhances the resilience of distributed intelligence networks against sophisticated, multi-vector attacks. The framework not only accurately isolates malicious actors with minimal latency but also exhibits tolerance toward benign nodes experiencing transient environmental disruptions, significantly lowering false positive rates. While the continuous evaluation of multidimensional risk introduces a slight computational overhead, the resultant stability and security heavily outweigh these operational costs. As digital infrastructure moves toward the era of 6G and ubiquitous decentralized intelligence, the adoption of dynamic, probabilistically driven trust frameworks will be essential. Future research should focus on optimizing the computational efficiency of the cross-layer risk evaluation algorithms and exploring the integration of advanced cryptographic primitives, such as zero-knowledge proofs, to further enhance privacy while maintaining rigorous risk calibration [31].

References

Tao, J., Lyu, R., & Cao, X. (2026). A Deep Learning-Based Automated Content Moderation Framework for Online Platforms.Future-Adaptive Intelligence and Lifelong Systems,1(1).

Li, X., Wang, P., Li, G., Ni, L., & Zhang, Y. (2023). Design of interface circuits and lightweight PUF for TMR sensors. IEEE Sensors Journal, 23(11), 11754-11761.

Tang M, Liu M, Li H, et al. Async learned user embeddings for ads delivery optimization[J]. arXiv preprint arXiv:2406.05898, 2024.

Liu, Fuqiang, and Sicong Jiang. "Temporally sparse attack for fooling large language models in time series forecasting." (2025).

Liao, Qiuyue, et al. "Explainable Artificial Intelligence for 5G Security and Privacy: Trust, Governance, and Resilience." (2025).

Lv, Qi, et al. "Spatial-temporal graph diffusion policy with kinematic modeling for bimanual robotic manipulation." Proceedings of the Computer Vision and Pattern Recognition Conference. 2025.

Yang, Z., Ji, W., Guo, Q., & Wang, Z. (2023, October). Javp: Joint-aware video processing with edge-cloud collaboration for dnn inference. In Proceedings of the 31st ACM International Conference on Multimedia (pp. 9152-9160).

Ma, Y., & Qu, D. (2026, February). IMFM-GNN: Interpretable Multimodel GNN Via Fourier-Markov Dynamics for Community Detection in Sustainable Energy Networks. In 2026 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA) (pp. 1-6). IEEE.

Ma, Y., Qu, D., & Wang, Y. (2026). HALO-GNN: hallucination-resistant temporal graph neural networks for dynamic community detection.Scientific Reports.

Zhang, W., Li, M., & Chen, X. (2026). Distributed Edge-Fog-Cloud Architecture for Intelligent Fault Diagnosis of Permanent Magnet Synchronous Motors Using Temporal Fusion Transformers and Federated Learning. Fundamental Scientific Reports in Multidisciplinary Areas, 2 (02), 121-131.

Yao, Y., Zhao, J., Li, Z., Cheng, X., & Wu, L. (2023). Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks. IEEE Transactions on Information Forensics and Security, 18, 1211-1224.

Qu, D., Ma, Y., & Wang, Y. (2026). STR-GNN: stability-regularized graph neural networks for suppressing spurious temporal variations in dynamic community detection. Scientific Reports.

Long, J., Xu, Z., Jiang, T., Yao, W., Jia, S., Ma, C., & Chen, X. (2025, April). Robust SAM: on the adversarial robustness of vision foundation models. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 39, No. 6, pp. 5775-5783).

Liu, Z., Qian, S., Cao, S., & Shi, T. (2025). Mitigating age-related bias in large language models: Strategies for responsible artificial intelligence development. INFORMS Journal on Computing.

Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. IEEE internet of things journal, 8(23), 16779-16786.

Chen, Q. (2026, February). Construction of a Blockchain and IoT-Based Cold Chain Logistics Data Security Traceability System. In2026 International Conference on Digital Analysis and Processing, Intelligent Computation (DAPIC)(pp. 396-399). The Academy of Engineering and Education.

Hu, S., Hu, X., & Ye, Q. (2017). Optimal rebate strategies under dynamic pricing. Operations Research, 65(6), 1546-1561.

Zhang, Q., Gao, W., Liu, C., Yao, Y., Yan, S., Shu, F., & Jin, S. (2025). Covert transmission for active RIS-aided full-duplex UAV integrated sensing, communication, and computation systems. IEEE Journal on Selected Areas in Communications.

Ma, Y., & Qu, D. (2026). Machine Learning Based Markov Decision Framework for Optimizing Circular Economy Systems.Engineering Proceedings,120(1), 44.

Wang Y, Fang Y, Wang T, et al. What Limits Vision-and-Language Navigation?[J]. arXiv preprint arXiv:2605.13328, 2026.

Yao, Y., Shu, F., Li, Z., Cheng, X., & Wu, L. (2023). Secure transmission scheme based on joint radar and communication in mobile vehicular networks. IEEE transactions on intelligent transportation systems, 24 (9), 10027-10037.

Qu, D., Ma, Y., Yan, J., & Pyrozhenko, M. (2026). TriMeta-BFNet: A Tri-Meta Stacked Atypical-Frequency Bayesian Fourier Neural Network for Hallucination-Resistant Community Detection. Mathematics, 14 (13), 2283.

Tao, J., Lyu, R., & Cao, X. (2026). A Scalable Data Governance Architecture for Privacy-Aware Intelligent Learning Systems in Lifelong. Future-Adaptive Intelligence and Lifelong Systems, 1 (1).

Wuyang Zhang and Shichao Pei. 2026. Your LLM Agent Can Leak Your Data: Data Exfiltration via Backdoored Tool Use. arXiv:2604.05432 [cs.CR] doi:10.48550/arXiv.2604.05432

Zhang, Y., Zhang, Y., Zhao, M., Feng, S., & Cheung, Y. M. (2026). How to Ask the AI: A User Perspective Survey for Large Language Model Prompting.IEEE Transactions on Artificial Intelligence.

Li, X., Wang, P., Li, G., & Zhang, Y. (2023). Design of a novel self-test-on-chip interface ASIC for capacitive accelerometers. IEEE Transactions on Circuits and Systems I: Regular Papers, 70(7), 2834-2843.

Wang, S., Zhang, X., Wang, P., & Li, X. (2026). Design of Magnetic Sensor Array-Based PUFs for IoT Security. IEEE Transactions on Instrumentation and Measurement, 75, 1-9.

Yang, Z., Ji, W., & Wang, Z. (2024). Adaptive joint configuration optimization for collaborative inference in edge-cloud systems. Science China Information Sciences, 67(4), 149103.

Zhao, Q., & Huang, Y. (2026). DAREA: A Dynamic AI-Driven Architecture for Real Estate Asset Tokenization on Blockchain.Fundamental Scientific Reports in Multidisciplinary Areas,2(02), 182-192.

Zhang, H., Zandsalimy, M., & Sushmita, S. (2026). Exposing LLM Safety Gaps Through Mathematical Encoding: New Attacks and Systematic Analysis.arXiv preprint arXiv:2605.03441.

Jin, H., Tsai, F. S., & Martinez-Vazquez, J. (2025). Optimal expenditure decentralization for sustainable development: evidence from a 52-country panel analysis. Financial Innovation, 11(1), 111.