Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Conceptual Framework for Secure and QoS-Aware IPv6 Networks Using Artificial Intelligence and Blockchain

Reema Roychaudhary

reema.roychaudhary@saii.siu.edu.in

Symbiosis International University

Research Article

Keywords: IPv6 Security, Quality of Service, Deep Reinforcement Learning, Blockchain Trust Management, Software-Defined Networking, Variational Autoencoder, IoT Routing, 6TiSCH, Explainable AI

Posted Date: June 26th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9767534/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Conceptual Framework for Secure and QoS-Aware IPv6 Networks Using Artificial Intelligence and Blockchain

Dr. Reema Roychaudhary
Symbiosis Artificial Intelligence Institute (SAII)
Symbiosis International Deemed University, Pune, Maharashtra, India
Email: reema.roychaudhary@saii.siu.edu.in

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices and the global transition toward IPv6-based infrastructures have introduced unprecedented complexity in ensuring network security, Quality of Service (QoS), and scalable trust management. Existing approaches, which independently employ either Artificial Intelligence (AI)-driven routing or blockchain-based security, fail to holistically address the intertwined challenges of resource constraints, dynamic network conditions, and sophisticated adversarial threats in heterogeneous IPv6 environments. This paper proposes a novel conceptual framework that synergistically integrates an AI-driven anomaly detection and trust evaluation engine with a lightweight blockchain ledger and a Deep Reinforcement Learning (DRL)-based QoS-aware routing module. The framework is architecturally partitioned into four coherent layers: (i) an IPv6 network infrastructure layer leveraging Software-Defined Networking (SDN) and IPv6 over the Time - Slotted Channel Hopping mode of IEEE 802.15.4e (6TiSCH); (ii) an AI-driven anomaly detection and trust evaluation layer employing Variational Autoencoders (VAE) and Artificial Neural Networks (ANN); (iii) a consortium blockchain secure ledger layer for immutable trust record management via smart contracts; and (iv) an intelligent QoS-aware routing engine based on Deep Q-Networks (DQN). The proposed conceptual integration addresses critical research gaps, including the absence of Explainable AI (XAI) in trust models, blockchain scalability in resource-constrained environments, cross-domain heterogeneity, and cold-start trust initialization. This paper presents a conceptual framework (Secure QoS- IPv6) to guide future implementation efforts. The framework is expected to significantly advance secure, adaptive, and efficient IPv6 network management in next-generation 6G and IoT ecosystems.

Keywords — IPv6 Security; Quality of Service; Deep Reinforcement Learning; Blockchain Trust Management; Software-Defined Networking; Variational Autoencoder; IoT Routing; 6TiSCH; Explainable AI.

I. INTRODUCTION

The Internet of Things (IoT) paradigm has catalyzed an exponential surge in network-connected devices, with global IoT connections projected to exceed 30 billion by 2030. This proliferation necessitates the adoption of IPv6 as the foundational protocol, given IPv4 exhaustion and the expansive address space IPv6 provides. However, the transition to large-scale IPv6 networks introduces multifaceted challenges spanning Quality of Service (QoS) assurance, intelligent routing, scalable trust management, and robust security — each of which is compounded by the inherent resource constraints of IoT and Wireless Sensor Network (WSN) nodes.

QoS optimization in IPv6 networks demands simultaneous satisfaction of conflicting objectives, including minimizing end-to-end delay, maximizing packet delivery ratio (PDR), ensuring energy efficiency, and maintaining throughput stability under dynamic and unpredictable traffic conditions. Traditional static routing protocols such as OSPF, AODV, and RPL are fundamentally ill-equipped to handle these demands in real time, as they rely on rule-based forwarding policies incapable of adapting to abrupt topology changes, link failures, or adversarial injection attacks. Moreover, conventional protocols implicitly trust neighboring nodes, rendering them vulnerable to routing-layer attacks, including black hole, sinkhole, wormhole, version number manipulation, and BGP prefix hijacking.

The emergence of Artificial Intelligence — in particular, Reinforcement Learning, Deep Learning, and bio-inspired optimization — offers a transformative paradigm for intelligent, adaptive routing and anomaly detection in IPv6 networks. Concurrently, blockchain technology provides a decentralized, tamper-resistant infrastructure for distributed trust management and secure node authentication. Despite their complementary strengths, the isolated application of either AI or blockchain to IPv6 network security has yielded only partial solutions. AI-based models remain opaque to network administrators and susceptible to adversarial

manipulation, while blockchain deployments suffer from prohibitive computational overhead, storage bloat, and consensus latency that conflict with the real-time demands of IoT environments.

This paper addresses these limitations by proposing a conceptual framework that unifies AI-driven anomaly detection, blockchain-secured trust management, and DRL-based QoS-aware routing into a cohesive, layered architecture for secure IPv6 networks. The primary objectives of this work are: (i) to identify and synthesize critical research gaps in existing AI-based and blockchain-based networking approaches; (ii) to design a conceptual four-layer architecture that integrates VAE/ANN-based anomaly detection, consortium blockchain with smart contract automation, and DQN-driven multi-objective routing; and (iii) to articulate the theoretical advantages of this integration and outline actionable future research directions.

This paper is conceptual in nature. Rather than presenting simulation results, our contribution is a novel architectural blueprint that synthesizes AI, blockchain, and QoS routing into a unified layered design. The framework is intended to inform and guide future prototype implementations in 6TiSCH and SDN testbeds.

The remainder of this paper is organized as follows. Section II presents a synthesis of related literature. Section III details the proposed conceptual framework. Section IV provides a comparative analysis. Section V outlines future research directions, and Section VI concludes the paper.

II. LITERATURE REVIEW

The existing body of literature on intelligent and secure IPv6 networking broadly partitions into three synergistic streams: AI-driven routing and QoS optimization, blockchain-based security and trust management, and hybrid AI-blockchain frameworks. The following subsections synthesize contributions within each stream, identify their strengths, and critically evaluate their limitations.

A. AI-Driven Routing and QoS Optimization

Reinforcement Learning (RL) techniques have gained considerable traction as adaptive routing mechanisms for dynamic IoT and vehicular networks. Q-learning has been employed to identify reliable routing paths in Software-Defined IoT (SD-IoT) environments, where the separation of the control and data planes enables centralized, intelligence-driven traffic management [1]. Deep Q-Networks (DQN) have been applied to Network Function Virtualization (NFV) placement at the edge, demonstrating superior throughput and delay performance relative to heuristic baselines [2]. Dynamic Objective Selection in Reinforcement Learning (DOS-RL) further extends conventional RL by employing shaped reward functions to accelerate convergence in multi-objective routing scenarios, simultaneously balancing energy consumption, latency, and PDR [1].

Beyond RL, bio-inspired meta-heuristic methods have been widely adopted for intelligent pathfinding. Ant Colony Optimization (ACO) has demonstrated effectiveness in low-power and lossy networks (LLNs) by emulating stigmergic pheromone trails to discover energy-efficient routes [5]. Hybrid approaches combining Grey Wolf Optimization and Artificial Democratic Cuckoo Glowworm Remora Optimization with routing protocols have reported accuracy rates approaching 96% in 6G security management scenarios [3]. For anomaly detection, Variational Autoencoders (VAEs) paired with attention mechanisms have been leveraged to extract deep spatio-temporal features of malicious routing behavior, outperforming traditional signature-based intrusion detection systems [2]. Artificial Neural Networks (ANN) have demonstrated high efficacy in detecting black hole attacks within Vehicular Ad Hoc Networks (VANETs), achieving detection accuracy of approximately 98.97% [7]. Nevertheless, the prevalent weakness across these approaches is their centralized vulnerability and the absence of a decentralized trust infrastructure to validate the integrity of AI model inputs themselves [4].

B. Blockchain-Based Security and Trust Management

Blockchain technology has emerged as a compelling mechanism for decentralized trust management in IPv6 and IoT networks [9]. Permissioned and consortium blockchains have been deployed to store node identities, Route Origin Authorization (ROA) records, and reputation scores immutably, thereby preventing BGP prefix hijacking and route manipulation [6]. Smart contracts have been integrated to automate node authentication and enforce access control policies without reliance on a centralized authority [9]. RSA-based cryptographic schemes combined with public-private blockchain architectures have shown the capability of eliminating malicious nodes while ensuring traceability and network lifetime extension in WSNs [6].

Despite these contributions, blockchain integration in resource-constrained IoT environments faces critical technical barriers. The computational overhead of consensus mechanisms, particularly Proof-of-Work, renders them infeasible for battery-powered sensor nodes [9]. Blockchain bloating — the accumulation of the full distributed ledger on each node — imposes severe storage overhead incompatible with embedded sensor memory [3]. Consensus latency conflicts with the real-time requirements of dynamic routing protocols such as BGP and VANET routing [6]. Furthermore, the lack of cross-domain interoperability standards leaves heterogeneous multi-domain IoT deployments vulnerable to white-washing attacks, where malicious nodes exploit domain transitions to evade trust penalties [8].

C. QoS-Aware Frameworks and Hybrid AI-Blockchain Approaches

Emerging research at the intersection of AI and blockchain has produced hybrid frameworks that leverage the complementary strengths of both paradigms. Feedforward Neural Networks (FNN) have been employed for global trust score computation, with results subsequently recorded on blockchain for tamper-proof, immutable storage [7]. Support Vector Regression (SVR) has been applied to predict link reliability metrics, feeding trust-aware routing decisions in SD-IoT architectures [1]. Enhanced AODV protocols augmented with clustering strategies and ANN-based threat classifiers have demonstrated reduced hop count and improved end-to-end delay in VANET environments [7]. In IPv6-over-TSCH (6TiSCH) deployments for industrial IoT, autonomous scheduling mechanisms have been proposed to ensure deterministic, low-latency communication suitable for mission-critical applications [4].

The critical shortcoming of existing hybrid frameworks is their treatment of blockchain as a static storage layer rather than an active execution environment. Smart contracts are infrequently exploited for real-time trust computation and automated enforcement [9]. Moreover, the cold-start problem — whereby newly joined nodes lack historical reputation data — remains inadequately addressed [8], as does the challenge of maintaining QoS optimization integrity under sparse or dishonest feedback conditions [3]. The absence of adversarial robustness mechanisms for AI-based routing models represents a further critical gap, as compromised VANET nodes can maliciously manipulate telemetry data to mislead ANN classifiers and DQN agents alike [7].

D. Research Gap Analysis

The synthesis of the reviewed literature reveals five principal research gaps, as depicted in Figure 1, that collectively motivate the integrated framework proposed in this paper:

- ***Explainability Deficit [2], [7]:*** Deep learning models, including VAE and ANN, achieve high detection accuracy but operate as black boxes, providing no interpretable rationale for trust decisions to network administrators — a critical barrier for operational deployment and regulatory compliance.
- ***Blockchain Scalability in Constrained Environments [3], [9]:*** Existing blockchain architectures impose prohibitive storage, latency, and energy overhead on IoT and WSN nodes, with no widely adopted lightweight alternative that preserves full auditability.
- ***Passive Blockchain Role [6], [9]:*** The majority of frameworks exploit blockchain solely as a static trust database, neglecting the potential of smart contracts for automated, real-time trust execution and dynamic policy enforcement.
- ***Cross-Domain Trust Deficiency [8]:*** Existing trust models are overwhelmingly designed for homogeneous single-domain networks, leaving multi-domain heterogeneous IPv6/IoT systems exposed to white-washing and domain-hopping adversaries.
- ***Cold-Start and Sparse Feedback [3], [8]:*** Mechanisms for bootstrapping trust for newly joined devices and handling dishonest or sparse feedback remain nascent and inadequately explored in the literature.

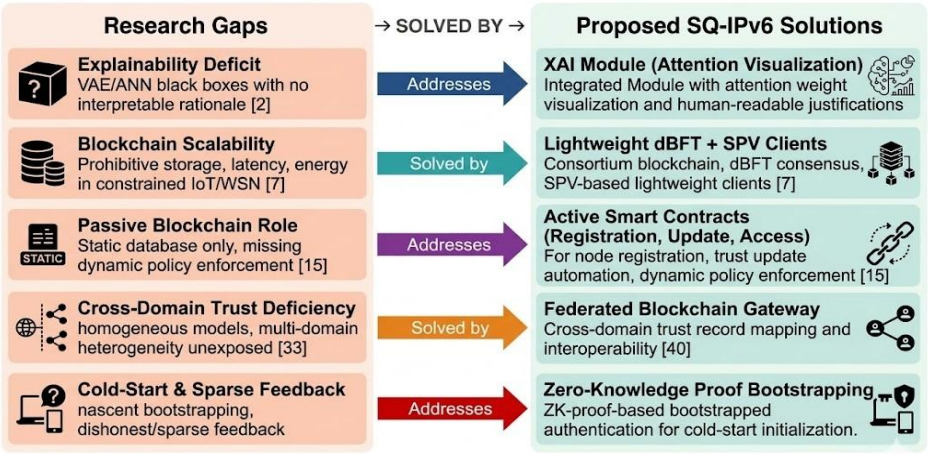


Fig.1 Research gap mapping and proposed SQ-IPv6 solutions

III. PROPOSED CONCEPTUAL FRAMEWORK

The proposed framework, designated SecureQoS-IPv6 (SQ-IPv6), is a four-layer conceptual architecture designed to holistically address secure, adaptive, and QoS-optimized routing in heterogeneous IPv6 networks. The architecture is illustrated conceptually in Figure 2 and described in detail in the following subsections. The framework is grounded in the principle of separation of concerns: each layer performs a well-defined function, while inter-layer communication follows a strictly defined data contract, ensuring modularity, scalability, and substitutability of individual components.

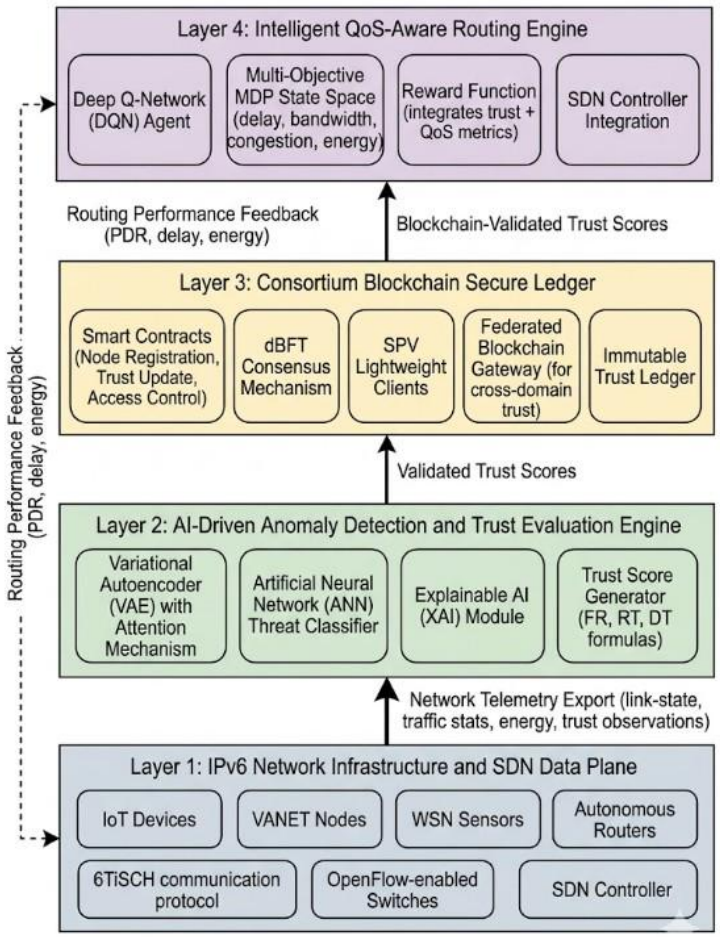


Fig.2 Layered Architecture of SQ-IPv6 Framework

A. Layer 1 — IPv6 Network Infrastructure and SDN Data Plane

The foundational layer encompasses the heterogeneous network of IoT devices, VANET nodes, WSN sensors, and autonomous system routers communicating over IPv6. 6TiSCH (IPv6 over Time-Slotted Channel Hopping MAC) is adopted for industrial IoT sub-networks, providing deterministic, low-latency communication suitable for real-time control applications. The Software-Defined Networking (SDN) paradigm governs the data plane, decoupling traffic forwarding from control logic. OpenFlow-enabled switches forward packets according to flow rules installed by the centralized SDN controller, which serves as the integration hub for AI and blockchain intelligence in higher layers.

This layer continuously exports network telemetry — including link-state advertisements, traffic flow statistics, node energy levels, and neighbor trust observations — to the AI-driven trust evaluation layer. The SDN architecture eliminates the per-node computational overhead of distributed routing computation, centralizing intelligence while preserving distributed data forwarding, a critical design principle for resource-constrained IoT environments.

B. Layer 2 — AI-Driven Anomaly Detection and Trust Evaluation Engine

Residing at the network edge or fog computing tier, this layer constitutes the analytical intelligence of the SQ-IPv6 framework. It ingests real-time telemetry from Layer 1 and performs two primary functions: behavioural anomaly detection and quantitative trust score computation.

A Variational Autoencoder (VAE) augmented with an attention mechanism is deployed for unsupervised anomaly detection. The VAE learns a probabilistic latent representation of normal network behavior from unlabeled telemetry data. Deviations from the learned distribution — quantified by the reconstruction error — trigger anomaly alerts. The attention mechanism enables the model to selectively weight the most informative telemetry features, improving sensitivity to sophisticated low-rate attacks. For classification of detected anomalies into specific attack categories (e.g., black hole, sinkhole, version number attack), an ANN classifier is employed, providing rapid, high-accuracy threat labelling.

Trust scores are computed as a composite function of three behavioral trust dimensions: forwarding reliability (FR), response trust (RT), and data trust (DT). These metrics are derived from historical interaction records, packet delivery observations, and anomaly detection outputs. The resulting trust scores are passed to Layer 3 for immutable recording and to Layer 4 for routing optimization.

The trust score $T(i,j)$ for node j as observed by node i is computed as follows in equation 1:

$$T(i,j) = w1 * FR(i,j) + w2 * RT(i,j) + w3 * DT(i,j) \qquad (1)$$

Where:

w – weight

FR- $FR(Forwarding\ Reliability) = \frac{successful_forwarded_packets}{total_packets_forwarded}$

RT- $RT(Response\ Trust) = \frac{successful_responses}{total_request_sent}$

DT- $DT(Data\ Trust) = 1 - \frac{\varepsilon}{\varepsilon_\max}$

where ε is the VAE reconstruction error, and ε_max is the maximum reconstruction error observed during training on benign network traffic (set to theoretically set to 1.0 where input features are normalized). DT ranges from 0 (fully anomalous) to 1 (fully trusted).

The weights satisfy $w1 + w2 + w3 = 1$, with $w1 = 0.4, w2 = 0.3,\ and\ w3 = 0.3$ (configurable based on network priorities). All trust scores are normalized to the range $[0,1]$.

An Explainability Module — a distinguishing novelty of this framework — generates human-readable justifications for each trust decision using attention weight visualization, enabling network administrators to audit and validate AI-driven conclusions, directly addressing the XAI research gap identified in Section II.

C. Layer 3 — Consortium Blockchain Secure Ledger

The blockchain layer provides decentralized, tamper-resistant storage and automated execution of trust-related operations. A consortium blockchain architecture is adopted, wherein computationally capable fog nodes and edge servers serve as validator peers, while resource-constrained IoT sensor nodes interact as lightweight clients using Simplified Payment Verification (SPV) — a mechanism that avoids full ledger storage and directly addresses the blockchain bloating problem. A delegated Byzantine Fault Tolerant (dBFT) consensus mechanism replaces energy-intensive Proof-of-Work, substantially reducing consensus latency and energy consumption to levels compatible with IoT operational constraints.

Smart contracts perform three critical automation functions within this layer: (i) Node Registration and Authentication — upon first network association, a new node undergoes a lightweight zero-knowledge proof-based credential verification, generating an initial bootstrapped trust score to mitigate the cold-start problem; (ii) Trust Score Update Automation — upon receipt of validated trust metrics from Layer 2, smart contracts atomically update the immutable trust ledger, ensuring consistency and preventing unauthorized modification; and (iii) Access Control Policy Enforcement — smart contracts dynamically revoke routing privileges from nodes whose trust scores fall below configurable thresholds, providing automated quarantine of malicious entities. Cross-domain interoperability is supported through a federated blockchain gateway that maps trust records across heterogeneous sub-domain blockchains, mitigating white-washing vulnerabilities.

D. Layer 4 — Intelligent QoS-Aware Routing Engine

The apex layer hosts the DRL-based routing decision engine, implemented as a Deep Q-Network (DQN) agent residing on the SDN controller. The DQN agent treats QoS-aware routing as a multi-objective Markov Decision Process (MDP), where the state space encodes real-time network conditions (link delay, bandwidth, congestion, node energy), the action space represents routing path selections, and the reward function integrates trust scores from Layer 3 with QoS metrics to produce a composite optimization signal.

The reward function is designed to simultaneously penalize routing through low-trust nodes, excessive energy consumption, high latency, and packet loss — balancing security and QoS objectives without manual parameter tuning.

The reward function $R(s,a)$for taking routing action a in state s is formally defined as in Equation 2:

$$R(s,a) = \alpha * PDR - \beta * Delay - \gamma * Energy + \delta * T_{avg} \qquad (2)$$

Where

PDR- Packet Delivery Ratio

$Delay$- Normalized latency

$Energy$- Residual Node Energy and,

T_avg- Average blockchain- validated trust score path.

The weights satisfy $\alpha + \beta + \gamma + \delta = 1, with\ \alpha = 0\ and\ \gamma = 0.2, and\ \delta = 0.3,$ aligning QoS and security objectives.

The DQN agent employs experience replay and a target network to stabilize training in the dynamic, non-stationary IPv6 network environment. Routing policies are periodically updated and installed as flow rules on SDN switches, ensuring that the network continuously adapts to evolving threat landscapes and traffic conditions. The integration of validated blockchain trust scores into the routing reward function ensures that routing decisions are simultaneously QoS-optimized and security-hardened — a synergy absent from all reviewed prior works.

E. Framework Workflow

The end-to-end data and control flow of the SQ-IPv6 framework proceeds as shown in Figure 3:

1. Network telemetry (link states, energy metrics, traffic flows) is continuously streamed from Layer 1 SDN-enabled nodes to the Layer 2 edge server.
2. The VAE anomaly detector processes the telemetry stream, computing reconstruction errors and flagging behavioral deviations. The ANN classifier labels detected anomalies by attack type.
3. The Explainability Module generates attention-weighted justifications for each trust evaluation, producing human-auditable reports.
4. Computed trust scores and anomaly labels are transmitted to Layer 3, where smart contracts atomically record them on the consortium blockchain ledger.
5. The Layer 4 DQN agent retrieves validated trust scores from the blockchain and current QoS metrics from the SDN controller, constructing the state vector for the routing MDP.
6. The DQN agent selects the optimal routing action, and the SDN controller installs the corresponding flow rules on network switches.
7. Routing performance feedback (PDR, delay, energy) is collected and fed back to the DQN agent as the environmental reward, completing the reinforcement learning cycle.

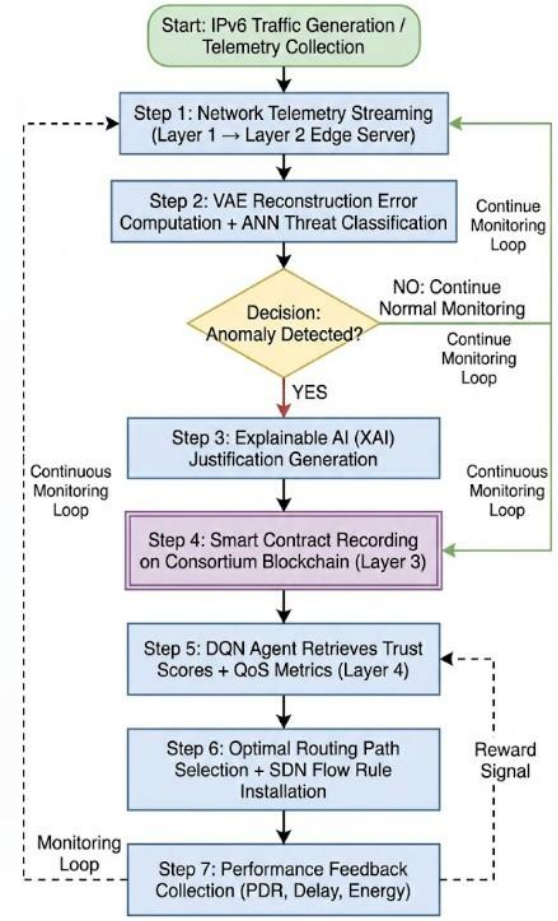


Fig.3 Operational workflow of the proposed SQ-IPv6 framework

IV. COMPARATIVE ANALYSIS

Table I presents a structured comparison of representative existing approaches against the proposed SQ-IPv6 framework across key technical dimensions. The analysis confirms that no existing work simultaneously addresses all five dimensions — QoS optimization, AI-driven anomaly detection, blockchain security, cross-domain trust, and XAI — that the proposed framework targets.

TABLE I — COMPARATIVE ANALYSIS OF EXISTING APPROACHES VS. PROPOSED FRAMEWORK

Approach	AI Technique	QoS Support	Blockchain Usage	XAI	Cross-Domain Trust	Key Limitation	Proposed Improvement
SD-IoT Reliable Path Prediction	SVR, Q-Learning	High	None	No	No	Centralized controller vulnerability; no decentralized trust	Blockchain-validated trust fed into DQN routing
Secure Satellite Routing (VAE)	VAE + Attention	High	None	No	No	High resource consumption; no cross-domain support	Lightweight consortium blockchain + federated gateway
Blockchain 6G Security (Remora)	Democratic Cuckoo RL	High	UDTP-RPR	No	No	Computationally demanding; no XAI transparency	XAI explainability module + dBFT consensus
VANET ANN Routing (Black Hole)	ANN Classifier	Medium	None	No	No	ANN weights susceptible to adversarial manipulation	Blockchain-immutable model anchoring + anomaly validation
Blockchain WSN Routing (RSA)	Trust FR, RT, DT	Medium	Public + Private	No	Partial	High RSA key generation latency; slow consensus	dBFT consensus + zero-knowledge proof bootstrapping
Secure BGP (Smart Contracts)	None	Low	Permissioned	No	No	Blockchain bloat; throughput constraints	SPV lightweight clients + sharded ledger design
Proposed SQ-IPv6 Framework	**VAE + ANN + DQN**	**High**	**Consortium + Smart Contracts**	**Yes**	**Yes**	**Conceptual stage; implementation pending**	**Unified four-layer AI + blockchain + QoS + XAI integration**

V. FUTURE RESEARCH DIRECTIONS

The SQ-IPv6 framework, while conceptually comprehensive, opens several critical avenues for future investigation that will be essential for its practical realization and extension.

- ***Explainable AI for Network Trust (XAI):*** Future work should develop domain-specific XAI techniques, such as SHAP-based feature attribution and counterfactual explanation generation, tailored to network telemetry data. Interpretable trust models would enable network operators to interrogate and validate AI-driven routing and security decisions, a prerequisite for regulatory compliance in critical infrastructure deployments.
- ***Edge-Federated and Sharded Blockchain Architectures:*** To overcome storage bloat and consensus latency without sacrificing auditability, research should explore federated learning combined with sharded off-chain storage architectures. Payment channel networks and state channel technologies from the cryptocurrency domain offer transferable insights for reducing on-chain transaction frequency in high-throughput IoT environments.
- ***Continuous State-Space Deep Reinforcement Learning:*** The DQN agent proposed herein operates on a discretized action space. Future extensions should investigate Deep Deterministic Policy Gradient (DDPG) and Proximal Policy Optimization (PPO) agents capable of continuous action selection, enabling finer-grained routing optimization in networks with fluid topology and traffic demands.
- ***Adversarial Robustness of AI Routing Models:*** The susceptibility of ANN and DQN agents to adversarial data injection — where compromised nodes deliberately manipulate telemetry to mislead routing decisions — remains critically underexplored. Future research should develop adversarial training regimes and certified robustness mechanisms specifically for network routing contexts.
- ***Adaptive Cold-Start Trust Initialization:*** Novel mechanisms leveraging federated reputation bootstrapping, incentive-compatible witness protocols, and zero-knowledge credential verification should be developed to assign reliable initial trust scores to newly joined devices without historical data.
- ***Digital Twin Integration for Proactive Optimization:*** Digital twin representations of physical IPv6 network nodes could enable predictive simulation of routing and security decisions before live deployment, reducing the risk of disruption and enabling proactive adaptation to anticipated network state changes.
- ***Scalable Cross-Domain IPv6 Security Frameworks:*** Standardized inter-blockchain communication protocols and cross-domain trust federation APIs should be formalized to enable seamless trust record exchange across heterogeneous sub-networks, directly mitigating white-washing attacks in multi-administrative-domain deployments.

VI. LIMITATIONS AND OPEN CHALLENGES

As a conceptual framework, SQ-IPv6 has several limitations that must be acknowledged before implementation:

A. **Absence of Empirical Validation**: The framework has not been implemented or tested in simulation or real-world enviro nments. Performance claims (e.g., detection accuracy, latency reduction, energy efficiency) remain theoretical and require e mpirical validation in future work.

B. **Computational Assumptions**: The framework assumes sufficient computational capacity at edge/fog nodes to run VAE i nference, DQN training, and blockchain consensus. Resource-constrained IoT devices themselves are not required to perfor m these operations, but the edge infrastructure must be provisioned accordingly.

C. **Consensus Centralization Trade-off**: The consortium blockchain with dBFT consensus assumes a trusted set of validato r nodes. In fully untrustworthy environments where validators may collude, security guarantees weaken. Future work should explore fully decentralized alternatives like Proof-of-Stake or DAG-based ledgers.

D. **DQN Convergence in Non-Stationary Environments**: Deep Q-Networks are known to experience convergence instabili ty when network conditions change rapidly. While experience replay and target networks mitigate this, no formal convergen ce guarantees are provided for highly dynamic IPv6 environments.

E. **Attack Model Scope**: The framework currently addresses routing-layer attacks (black hole, sinkhole, version number). Ph ysical-layer jamming, side-channel attacks, and advanced persistent threats (APTs) are outside the current scope.

F. **Cross-Domain Gateway Specification**: The federated blockchain gateway for cross-domain trust transfer remains unders pecified. Practical implementation would require standardized inter-blockchain communication protocols (e.g., Polkadot's X CMP, Cosmos IBC).

These limitations do not invalidate the conceptual contribution but instead define clear boundaries and priorities for future re search.

VII. CONCLUSION

This paper has presented SQ-IPv6, a novel conceptual framework for secure, QoS-aware IPv6 networking that synergistically integrates AI-driven anomaly detection, blockchain-secured distributed trust management, and Deep Reinforcement Learning-based adaptive routing. Motivated by the demonstrated inadequacies of existing AI-only and blockchain-only approaches — particularly their failure to simultaneously address QoS optimization, transparent trust evaluation, cross-domain interoperability, and resource-constrained deployability — the framework introduces a four-layer architecture in which each component addresses a specific, well-defined technical challenge.

The conceptual contributions of this work are threefold. First, the integration of a VAE-based anomaly detector with an ANN classifier and an Explainability Module constitutes, to the best of the authors' knowledge, the first XAI-enabled trust evaluation pipeline explicitly designed for IPv6 network routing contexts. Second, the adoption of a consortium blockchain with dBFT consensus and SPV-based lightweight client participation directly addresses blockchain scalability and energy constraints without compromising auditability. Third, the use of blockchain-validated trust scores as direct inputs to the DQN routing reward function establishes a principled, verifiable linkage between security state and routing decisions — a novel architectural coupling absent from the existing literature.

The practical impact of the proposed framework extends beyond theoretical elegance. In the rapidly evolving context of 6G IoT networks, autonomous vehicles, and critical infrastructure interconnection over IPv6, the ability to deliver simultaneously secure, efficient, and interpretable network management constitutes an essential

capability. The SQ-IPv6 framework provides a principled architectural blueprint toward this goal, with clearly defined implementation pathways and research priorities outlined in Section V.

Future work will focus on prototype implementation within a 6TiSCH and SDN testbed environment, empirical validation of the XAI trust module, and performance benchmarking of the DQN routing engine under realistic adversarial network conditions.

ACRONYMS

6TiSCH	IPv6 over Time-Slotted Channel Hopping MAC
ANN	Artificial Neural Network
dBFT	delegated Byzantine Fault Tolerant
DQN	Deep Q-Network
DRL	Deep Reinforcement Learning
FR	Forwarding Reliability
IoT	Internet of Things
MDP	Markov Decision Process
PDR	Packet Delivery Ratio
QoS	Quality of Service
SDN	Software- Defined Networking
SPV	Simplified Payment Verification
VAE	Variational Autoencoder
XAI	Explainable Artificial Intelligence
RT	Response Trust

REFERENCES

[1] M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996-2018, 2014.

[2] V. Mnih et al., "Human-Level Control Through Deep Reinforcement Learning," Nature, vol. 518, no. 7540, pp. 529–533, Feb. 2015.

[3] Y. Liu, J. Yu, J. Kang, D. Niyato, and S. Xie, "Blockchain-Empowered Secure Federated Learning for 6G IoT: Architecture, Challenges, and Solutions," IEEE Network, vol. 36, no. 3, pp. 128-135, 2022.

[4] T. Watteyne et al., "6TiSCH: From Niche Industrial Scenario to Generic IoT Networking," in Proc. European Wireless (EW) Conf., Barcelona, Spain, 2014, pp. 1–6.

[5] M. Dorigo and T. Stutzle, Ant Colony Optimization. Cambridge, MA, USA: MIT Press, 2004.

[6] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for Industry 4.0: A Comprehensive Review," IEEE Access, vol. 8, pp. 79764-79800, 2020.

[7] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," IEEE Signal Processing Magazine, vol. 36, no. 5, pp. 41-49, 2019.

[8] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, S. Sheng, and J. Yu, "Attacks and Defences on Intelligent Connected Vehicles: A Survey," Digital Communications and Networks, vol. 6, no. 4, pp. 399–421, Nov. 2020.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[10] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2961–2991, 2018.

Funding

No funding was received for this work.