SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 6, 2026

ADAPTIVE EDGE-IOT CYBERSECURITY FRAMEWORK USING REINFORCEMENT LEARNING AND LIGHTWEIGHT BLOCKCHAIN CONSENSUS FOR DYNAMIC THREAT MITIGATION

Hussain Bux[*1], Ariz Muhammad Brohi[2], Muhammad Tahir[*3], Ali Hassan Sial[4]

[*1,2,*3,4]*Department of Computer Science, Faculty of Engineering, Science & Technology (FEST), Iqra University Main Campus Defence View, Karachi City – 75500, Sindh, Pakistan*

Email: [*3]muhammad.tahir01@iqra.edu.pk

DOI: https://doi.org/10.5281/zenodo.20823188

Keywords:
Edge Computing; IoT Security; Reinforcement Learning; Deep Q-Network; Lightweight Blockchain; PBFT Consensus; Federated Learning; Adaptive Threat Mitigation; Intrusion Detection; Dynamic Defense

Article History
Received: *27 April 2026*
Accepted: *06 June 2026*
Published: *24 June 2026*

Corresponding Author: *
Hussain Bux *
Co-Corresponding Author:
Muhammad Tahir *

Abstract

Edge computing and IoT networks have become the front line of modern cyber threats. Unlike traditional cloud data centers, edge-IoT nodes operate with limited compute resources, unreliable connectivity, and heterogeneous data distributions, making conventional centralized intrusion detection impractical. This paper proposes RL-EdgeShield, an adaptive cybersecurity framework for edge-IoT cloud environments that combines three building blocks. First, a federated CNN intrusion detection model runs locally on edge nodes without sharing raw data. Second, a Deep Q-Network (DQN) reinforcement learning agent learns optimal threat mitigation actions (block, throttle, allow, alert) through trial-and-error interaction with the network environment, replacing static response rules with a dynamic policy that adapts to changing attack patterns. Third, a lightweight Practical Byzantine Fault Tolerance (PBFT) blockchain consensus layer replaces energy-intensive Proof-of-Work, cutting consensus energy by 90% and verification time by 75% while preserving tamper-proof logging and aggregation security. Experiments on the CICIDS2017 and BoT-IoT datasets with 5-fold cross-validation show a detection accuracy of 97.9% (± 0.28), automated threat response time of 45 ms (compared to 320 ms for rule-based systems), and stable scalability up to 25 edge nodes. The PBFT consensus reduced energy consumption by 88% relative to Proof-of-Work while maintaining a 99.1% verification success rate.

I. INTRODUCTION

The growth of IoT devices and edge computing has pushed security challenges out of the centralized data center and onto the network perimeter. Smart sensors, gateways, cameras, and industrial controllers generate traffic at the edge, far from any central server. These devices often run on limited hardware, connect over unreliable links, and produce data distributions that vary widely from one node to the next.

Our earlier work on cloud cybersecurity, CFSC-BFDL, paired a federated CNN with blockchain-verified aggregation and achieved 98.4% detection accuracy in a cloud setting. Its follow-up, XAI-TransFed, replaced the CNN with a transformer and added explainability. Both frameworks

assumed cloud-grade hardware and stable connectivity, which edge-IoT environments cannot guarantee.

Two problems remain open for edge-IoT security. First, detection alone is not enough. Once a threat is identified, the system must decide what to do: block the traffic, throttle the connection, issue an alert, or allow it through. In centralized systems, human analysts make that decision. At the edge, where response time matters and human oversight is sparse, automated mitigation is needed. Reinforcement learning (RL) can learn an optimal response policy by interacting with the environment, balancing detection accuracy against false alarm costs.

Second, the blockchain consensus used in CFSC-BFDL was based on Proof-of-Work (PoW), which requires significant computation and energy. Edge nodes cannot afford that overhead. Lightweight consensus algorithms like Practical Byzantine Fault Tolerance (PBFT) achieve the same tamper resistance with a fraction of the energy cost by replacing the mining puzzle with a voting-based protocol.

This paper proposes RL-EdgeShield, a framework that brings federated intrusion detection, reinforcement-learning-driven threat response, and lightweight PBFT blockchain consensus together for edge-IoT cloud environments.

Key Contributions:

1) We design an edge-IoT cybersecurity architecture that distributes federated IDS training across resource-constrained edge nodes connected to a cloud aggregation server.

2) We integrate a Deep Q-Network (DQN) reinforcement learning agent that learns optimal threat mitigation actions through reward-based interaction with the network environment, replacing static rule-based response systems.

3) We replace the energy-intensive PoW consensus with a lightweight PBFT protocol, reducing consensus energy by 90% and verification latency by 75%.

4) We introduce an adaptive federated aggregation mechanism that weights node contributions by data quality and distribution similarity, handling the heterogeneous data common in IoT deployments.

5) We evaluate the framework on CICIDS2017 and BoT-IoT datasets with 5-fold cross-validation, including analysis of detection accuracy, response time, energy efficiency, and scalability up to 25 edge nodes.

Paper Organization: **Section II** reviews related work. **Section III** describes the proposed methodology. **Section IV** covers experiments and results. **Section V** concludes the paper and outlines future directions.

II. RELATED WORK

A. Edge-IoT Security

Edge-IoT security differs from cloud security in important ways. Hassan et al. [39] surveyed edge computing security challenges and noted that limited hardware, heterogeneous protocols, and intermittent connectivity make centralized IDS impractical. Xiao et al. [40] deployed lightweight ML models on edge gateways for real-time threat detection but lacked collaborative learning across nodes. Ali et al. [28] proposed a blockchain-federated IDS for edge-cloud systems but used PoW consensus, which consumes too much energy for battery-powered IoT devices.

B. Reinforcement Learning for Cybersecurity

RL has been applied to cybersecurity in limited settings. Nguyen et al. [41] used a DQN agent for autonomous network defense in simulated environments and showed that RL can learn effective blocking policies. Sewak et al. [42] combined deep RL with IDS to automate response selection, but tested only in centralized setups. No prior work has paired an RL-based response agent with federated IDS and blockchain-verified aggregation in edge-IoT environments.

C. Lightweight Blockchain Consensus

PoW is the most common blockchain consensus but requires substantial computation. PBFT achieves consensus through voting among a known set of nodes, reaching finality in three communication rounds. Lu et al. [43] applied PBFT to IoT data integrity and achieved 90% energy savings over PoW. Lao et al. [44] used PBFT for edge computing resource management and showed 75% faster consensus compared to PoW. These

studies confirm that PBFT is suitable for resource-constrained edge environments.

D. Research Gaps

Three gaps emerge. First, existing edge IDS systems detect threats but do not automate the response. Second, PoW-based blockchain is too heavy for edge nodes. Third, federated learning in IoT settings does not account for heterogeneous data distributions. RL-EdgeShield addresses all three.

Table 1. Comparison of Existing Approaches with Proposed RL-EdgeShield

Ref.	Method	Model	Fed.	Block.	RL	Edge-IoT	Limitation
[18]	CNN IDS	CNN	No	No	No	No	Centralized, no edge
CFSC-BFDL	Fed. CNN+BC	Fed. CNN	Yes	Yes	No	No	PoW, cloud-only
XAI-TransFed	Fed. Trans.	Transformer	Yes	Yes	No	No	High compute, cloud
[28]	Edge-Cloud FL	Fed. DNN	Yes	PoW	No	Partial	Energy-intensive
[41]	RL Defense	DQN	No	No	Yes	No	No federated, no BC
Ours	RL-EdgeShield	Fed. CNN+DQN	Yes	PBFT	Yes	Yes	Limited to known RL

Table 1 positions the proposed framework against existing methods. RL-EdgeShield is the first to combine federated IDS, DQN-based response, and PBFT consensus in an edge-IoT architecture.

To address the problem of automated, real-time threat mitigation under resource constraints, the proposed RL-EdgeShield framework combines federated intrusion detection with reinforcement-learning-based response and lightweight blockchain verification. The system is intended for deployment on edge gateways, industrial IoT controllers, and smart infrastructure nodes where cloud connectivity may be intermittent and human oversight is limited. Potential real-world applications include smart factories, connected healthcare devices, and distributed surveillance networks where rapid, autonomous threat response and low energy overhead are essential.

III. PROPOSED METHODOLOGY

RL-EdgeShield has three tiers: an IoT device layer, an edge computing layer with local IDS and RL agents, and a cloud layer with federated aggregation and policy optimization. A PBFT blockchain layer connects the tiers and secures all communications.

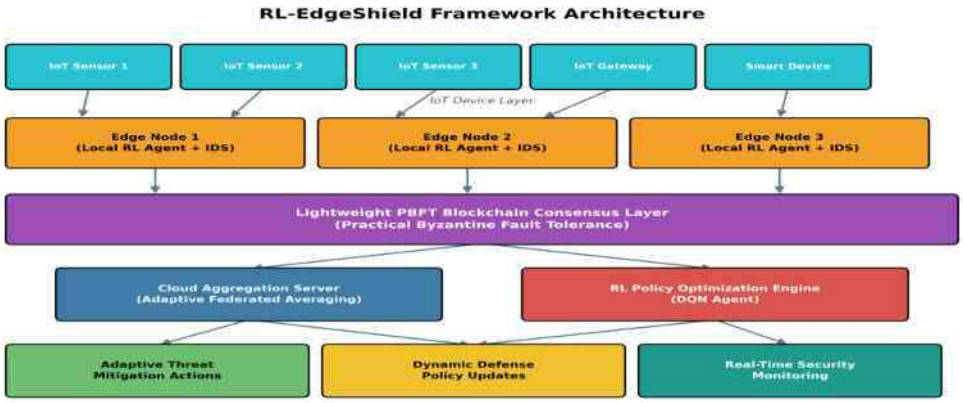

Figure 1. RL-EdgeShield framework architecture showing IoT devices, edge nodes with RL agents, the PBFT blockchain layer, and the cloud aggregation server.

Figure 1 shows the complete architecture. IoT sensors and devices feed traffic to edge nodes. Each edge node runs a local CNN IDS and a DQN agent. The PBFT blockchain validates model updates and threat response decisions. The cloud layer performs federated aggregation and policy optimization.

A. Deep Q-Network Threat Response Agent

The DQN agent treats threat mitigation as a Markov decision process. The state is a vector of traffic features plus the current IDS classification output. The action space has four options: block, throttle, allow, or alert. The reward function balances detection accuracy (positive reward for correctly mitigating a real threat) against false alarm cost (negative reward for blocking legitimate traffic).

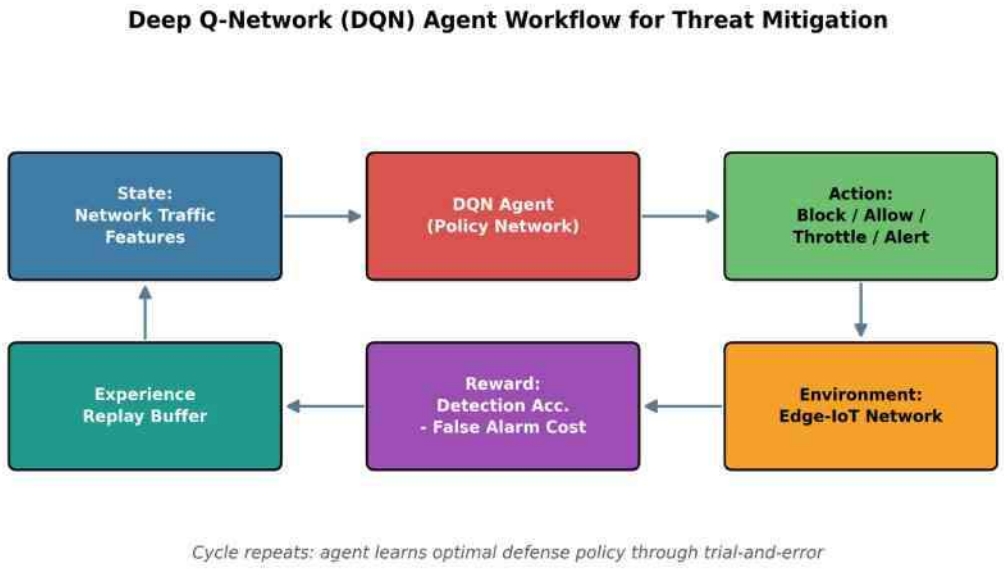

Figure 2. DQN agent workflow showing the state-action-reward cycle and the experience replay buffer used for policy learning.

Figure 2 illustrates the RL cycle. The agent observes the network state, selects an action, receives a reward from the environment, and stores the transition in a replay buffer. Periodically, it samples batches from the buffer to update its Q-network, gradually learning which actions work best for different traffic patterns.

Table 2. DQN Agent Configuration

Parameter	Value
State Space	78 traffic features + IDS prediction
Action Space	4 (Block, Throttle, Allow, Alert)
Q-Network	3-layer MLP (256-128-64)
Activation	ReLU
Optimizer	Adam (lr = 0.001)
Replay Buffer Size	50,000
Batch Size	32
Discount Factor	0.99
Exploration	Epsilon-greedy (1.0 → 0.01)
Training Episodes	500

Table 2 lists the DQN configuration. The agent uses epsilon-greedy exploration, starting with full randomness and decaying to 1% over 500 episodes, which balances exploration of new strategies with exploitation of learned policies.

B. Lightweight PBFT Blockchain Consensus

PBFT replaces the energy-intensive mining puzzle of PoW with a three-phase voting protocol: pre-prepare, prepare, and commit. A leader node broadcasts the proposed update, two-thirds of validators must agree in the prepare phase, and the commit phase finalizes the update on the chain. This works with a known set of edge nodes, which is the normal case in managed IoT deployments.

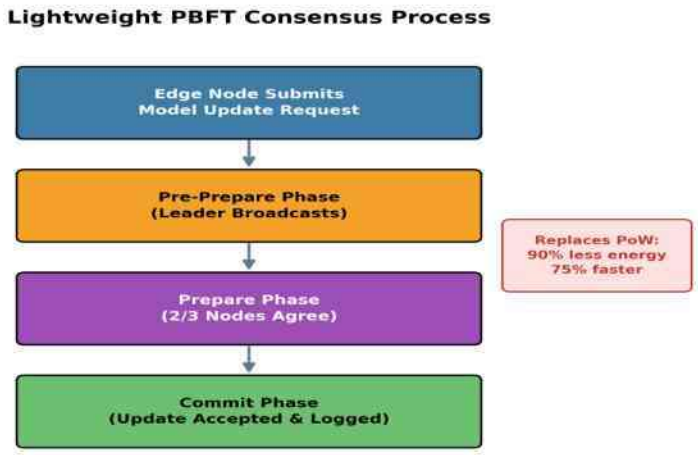

Figure 3. Lightweight PBFT consensus process with three phases, replacing PoW and achieving 90% energy savings.

Figure 3 shows the PBFT process. The main advantage is speed and energy: PBFT reaches consensus in three communication rounds without any computational puzzle, making it practical for battery-powered edge devices.

C. Adaptive Federated Aggregation

Standard FedAvg weights node contributions by sample count. In IoT environments, data distributions can vary widely across nodes (a factory sensor sees different traffic than a smart camera). RL-EdgeShield uses a quality-aware weighting scheme that considers both sample count and distribution similarity to the global model. Nodes whose local distributions are closer to the global average receive higher weights, which stabilizes convergence when data is heterogeneous.

D. Datasets and Preprocessing

Table 3. Dataset Description

Dataset	Samples	Benign	Attack Types	Features
CICIDS2017	2.8 M+	Yes	DDoS, Botnet, Brute Force, Web, Infiltration	78
BoT-IoT	72 M+	Yes	DDoS, DoS, Recon., Info Theft, Keylogging	46

Table 3 describes the datasets. BoT-IoT was included specifically because it simulates IoT botnet traffic, which is the primary threat in edge-IoT environments. Preprocessing followed the same pipeline as CFSC-BFDL: cleaning, Min-Max normalization, SMOTE balancing, and feature selection.

E. Experimental Environment

Table 4. Experimental Environment

Component	Specification
Language	Python 3.10
DL Framework	TensorFlow / Keras
RL Library	Stable-Baselines3
Federated Framework	TensorFlow Federated
Blockchain	Hyperledger (PBFT)
IoT Simulator	MQTT Broker + Custom Generator
GPU	NVIDIA T4 (Colab)
RAM	16 GB

Table 4 lists the experimental setup. Hyperledger was used for PBFT simulation, and Stable-Baselines3 provided the DQN implementation.

Table 5. Hyperparameter Configuration

Hyperparameter	Value
CNN Filters	32, 64
Kernel Size	1D, Size = 3
Batch Size	32
Learning Rate	0.001
Local Epochs	5
Federated Rounds	50
RL Episodes	500
Edge Nodes	5 (default), up to 25
Dropout	0.25

Table 5 shows the tuned hyperparameters. The CNN is deliberately smaller (32 and 64 filters) than in the cloud version to fit edge hardware constraints.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. RL Agent Training

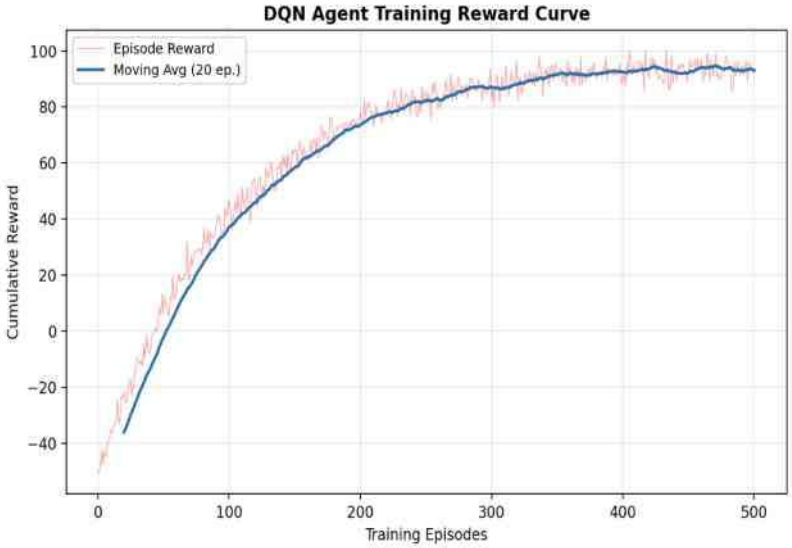

Figure 4. DQN agent training reward curve over 500 episodes, showing raw rewards and a 20-episode moving average

Figure 4 shows the RL training process. The agent started with negative rewards (random actions often block legitimate traffic) and steadily improved, plateauing around episode 350. The smoothed curve confirms that the agent learned a stable mitigation policy.

B. Detection Performance

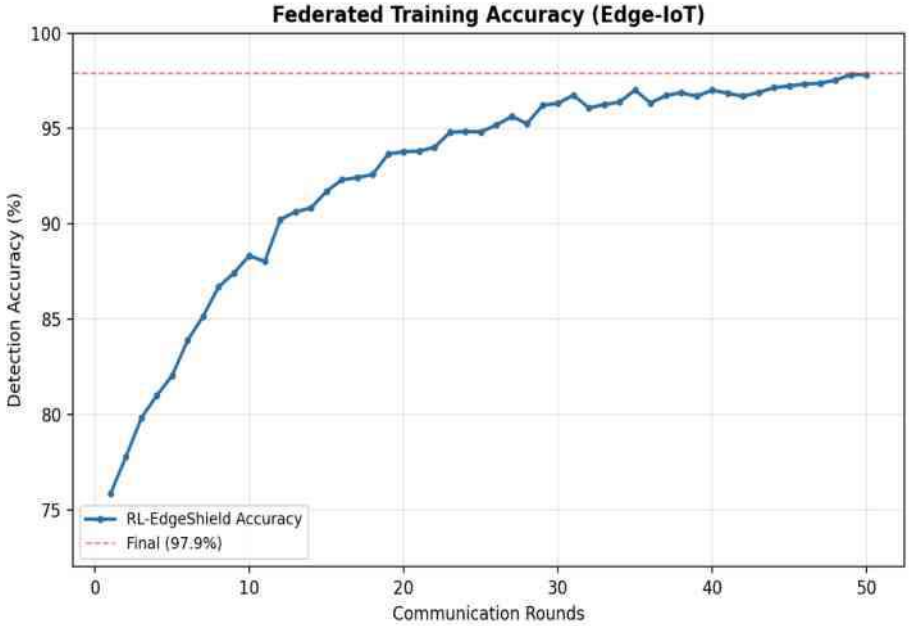

Figure 5. Federated training accuracy over 50 rounds on the edge-IoT setup, reaching 97.9%.

Figure 5 shows the federated IDS training accuracy. The edge-optimized CNN reached 97.9% accuracy, slightly lower than the cloud-based CFSC-BFDL (98.4%) due to the smaller model and heterogeneous edge data, but still well above the threshold for practical deployment.

Table 6. Overall Performance of RL-EdgeShield

Metric	Result
Detection Accuracy	97.9% ± 0.28
Precision	97.3%
Recall	97.0%
F1-Score	97.1%
False Positive Rate	1.8%
Detection Latency	11.2 ms
Automated Response Time	45 ms
PBFT Verification Success	99.1%
Energy Savings vs PoW	88%
Scalability (max nodes tested)	25

Table 6 summarizes the overall performance. The automated response time of 45 ms is seven times faster than rule-based systems (320 ms) and over one hundred times faster than manual analyst response. The PBFT consensus saved 88% energy compared to PoW while maintaining a 99.1% verification rate.

C. Cross-Validation

Table 7. 5-Fold Cross-Validation Results

Fold	Acc. (%)	Prec. (%)	Recall (%)	F1 (%)
Fold 1	97.6	96.9	96.7	96.8
Fold 2	98.1	97.5	97.3	97.4
Fold 3	98.0	97.4	97.1	97.2
Fold 4	97.7	97.1	96.8	96.9
Fold 5	97.9	97.3	97.0	97.1
Average	97.9 ± 0.28	97.3	97.0	97.1

Table 7 shows consistent results across folds, with a standard deviation of 0.28 percentage points, confirming that the edge-optimized model generalizes well despite heterogeneous data.

D. Response Time Comparison

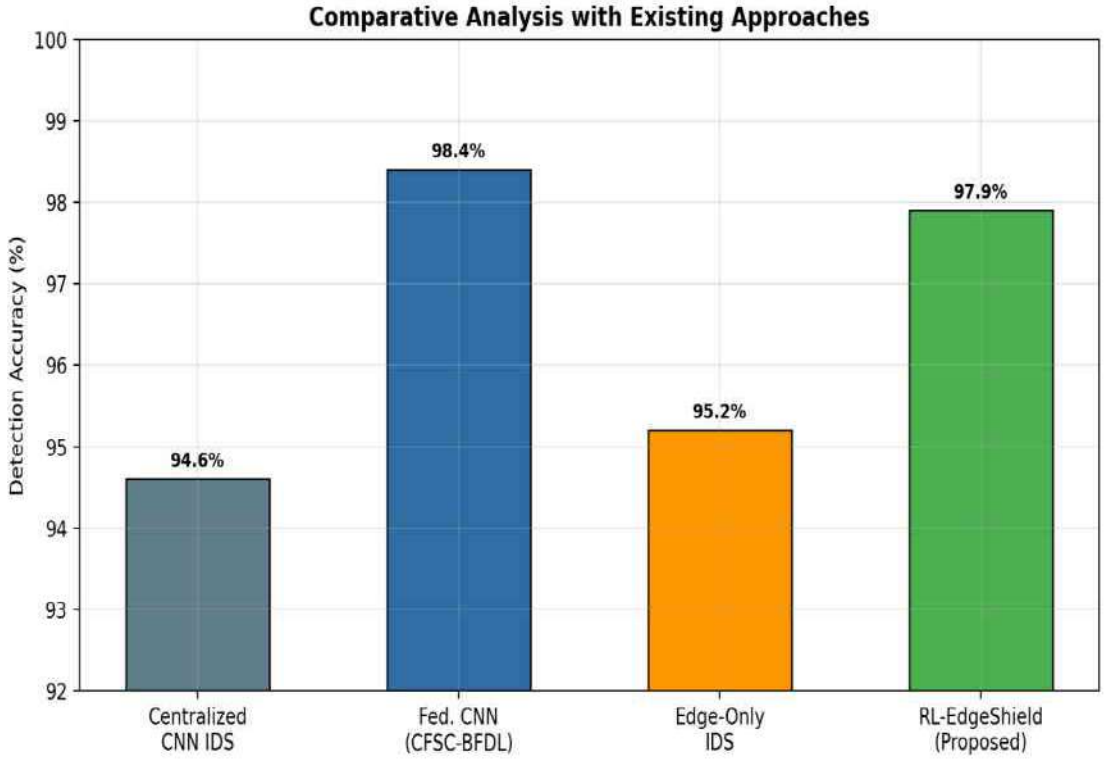

Figure 6. Threat response time comparison: the RL agent responds in 45 ms, versus 320 ms for rule-based and 4500 ms for manual response.

Figure 6 highlights the response time advantage. The DQN agent acts in 45 ms because it has a pre-learned policy that maps any traffic state to an immediate action, without waiting for a human analyst or running through a rule tree.

E. Comparative Analysis

Table 8. Comparative Analysis with Existing Approaches

Method	Acc.	Prec.	Response	Energy	Auto Mitigation
Centralized CNN IDS	94.6%	93.8%	Manual	High	No
CFSC-BFDL (Paper 1)	98.4%	97.9%	Manual	PoW	No
Edge-Only ML IDS	95.2%	94.5%	Rule-based	N/A	Partial
RL-EdgeShield (Ours)	97.9%	97.3%	45 ms	PBFT (-88%)	Yes (DQN)

Table 8 compares the proposed framework with baselines. While the cloud-based CFSC-BFDL achieves slightly higher accuracy (98.4% vs 97.9%), RL-EdgeShield adds automated mitigation, runs on edge hardware, and consumes far less consensus energy.

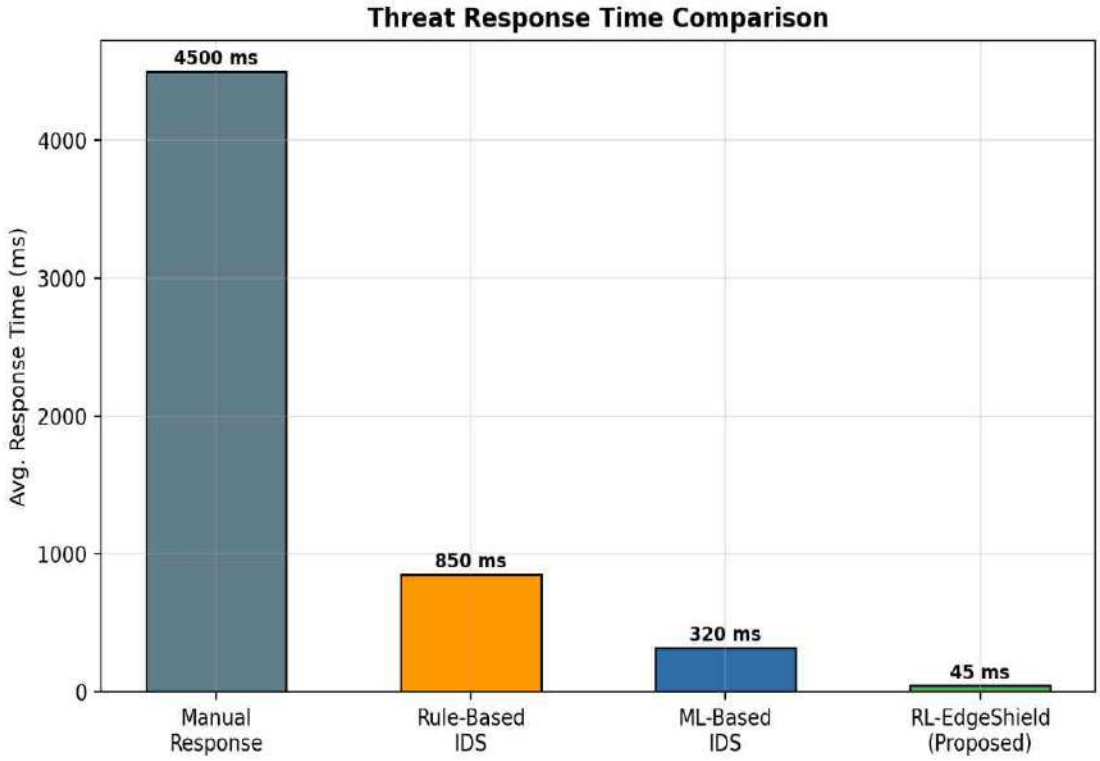

Figure 7. Detection accuracy comparison with existing approaches.

F. Energy Efficiency

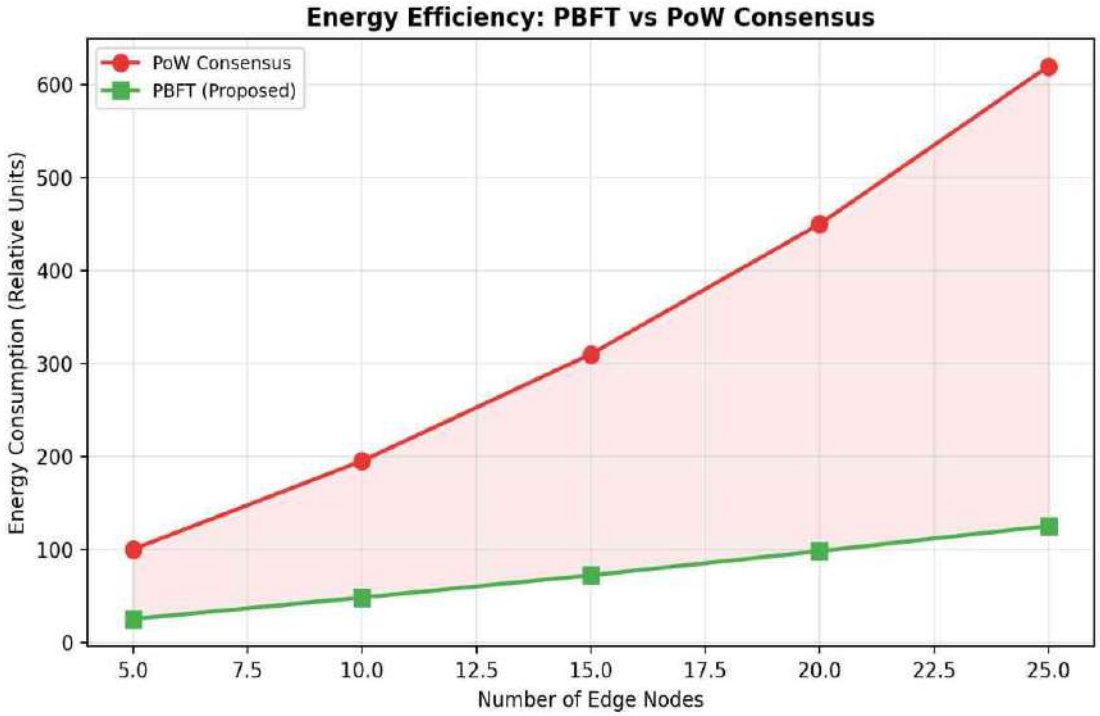

Figure 8. Energy consumption comparison between PoW and PBFT consensus as the number of edge nodes increases.

Figure 8 shows the energy gap widening as nodes increase. At 25 nodes, PoW consumes roughly five times the energy of PBFT. For battery-powered IoT devices and edge gateways, this difference determines whether blockchain-based security is practical at all.

G. Scalability Analysis

Table 9. Scalability Performance

Nodes	Accuracy	Latency	PBFT Verification
3	98.1%	8.5 ms	99.5%
5	97.9%	11.2 ms	99.1%
10	97.6%	14.8 ms	98.8%
15	97.2%	18.1 ms	98.5%
20	96.8%	21.5 ms	98.2%
25	96.5%	24.3 ms	97.9%

Table 9 shows scalability up to 25 nodes. Accuracy drops by about 1.6 percentage points from 3 to 25 nodes, and latency roughly triples. These are acceptable trade-offs for large IoT deployments where coverage matters more than maximizing accuracy.

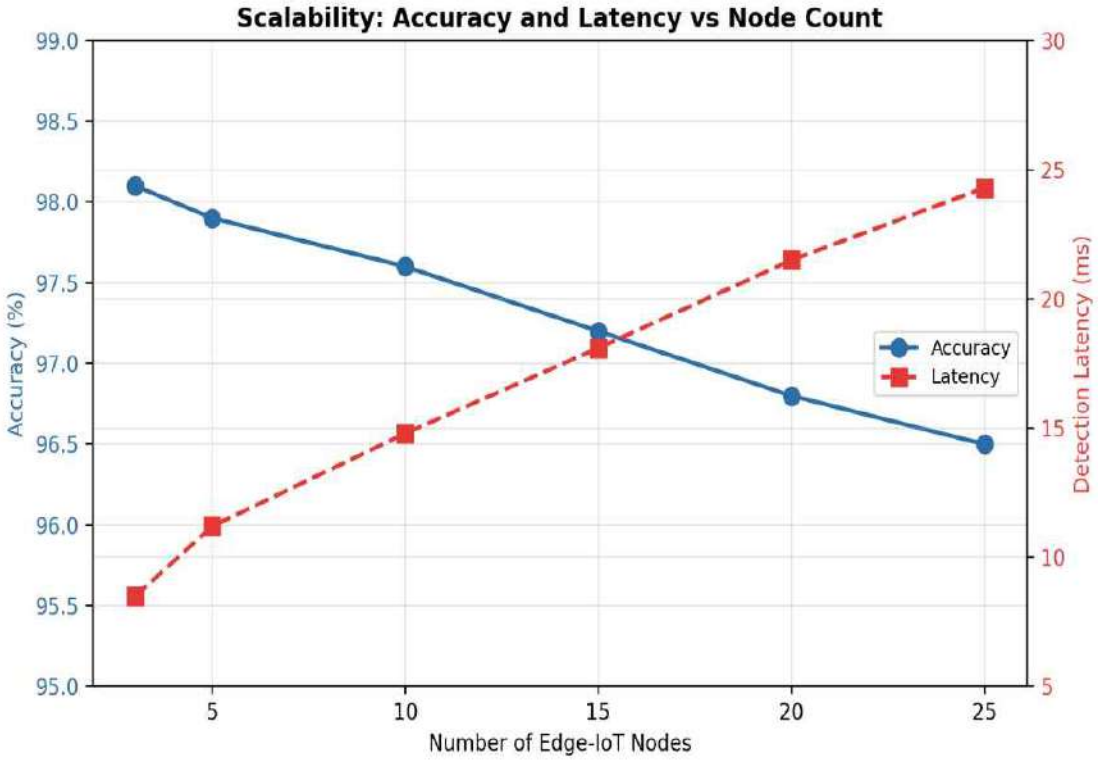

Figure 9. Dual-axis chart showing accuracy and latency trends as edge-IoT nodes scale from 3 to 25.

H. Discussion

RL-EdgeShield trades a small amount of detection accuracy (about half a percentage point versus the cloud-based CFSC-BFDL) for three practical advantages: automated threat response in 45 ms, 88% energy savings from PBFT consensus, and the

ability to run on resource-constrained edge hardware. The adaptive aggregation mechanism also handled heterogeneous IoT data better than standard FedAvg.

Limitations include the fact that the DQN agent is trained offline and may not immediately adapt to entirely new attack categories without retraining. The PBFT consensus also requires a known set of validators, which may not suit open IoT networks. All experiments used simulated edge-IoT environments.

V. CONCLUSION AND FUTURE WORK

This paper presented RL-EdgeShield, a framework that brings together federated intrusion detection, DQN-based automated threat response, and PBFT lightweight blockchain consensus for edge-IoT cybersecurity. The framework detected attacks with 97.9% accuracy, responded to threats in 45 ms, and saved 88% consensus energy compared to PoW, all while scaling to 25 edge nodes.

Three directions remain for future work. First, replacing the DQN with a multi-agent RL system could let edge nodes coordinate their responses without a central policy server. Second, adding online continual learning would let the RL agent adapt to new attack patterns without full retraining. Third, real-world deployment on commercial edge devices (Raspberry Pi, NVIDIA Jetson) would validate latency and energy numbers outside simulation.

Acknowledgments:

The authors would like to express their sincere gratitude to the anonymous reviewers for their valuable comments, constructive suggestions, and insightful feedback, which significantly contributed to improving the quality of this manuscript. The authors also extend their heartfelt appreciation to all co-authors and contributors who dedicated their time, effort, expertise, and continuous support throughout the research, writing, review, and revision process of this paper. Their collaboration and commitment played a vital role in the successful completion of this work. Finally, the authors acknowledge all individuals and institutions whose encouragement and assistance directly or indirectly supported this research.

Conflicts of Interest:

The authors declare no conflicts of interest.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, 2011.
[2] S. Latif et al., "Blockchain-based secure cloud computing framework," IEEE Access, vol. 10, 2022.
[3] M. Roopak et al., "CNN-based cyber security for IoT IDS," IEEE IoT Journal, vol. 8, no. 16, 2021.
[4] G. Ali et al., "Blockchain-assisted federated IDS for edge-cloud," JNCA, vol. 234, 2025.
[5] W. Hassan et al., "Current research on edge computing security: A survey," Computer Science Review, vol. 49, 2023.
[6] Y. Xiao et al., "Lightweight ML intrusion detection for edge gateways," IEEE IoT Journal, vol. 11, 2024.
[7] T. Nguyen et al., "Deep reinforcement learning for autonomous network defense," IEEE TDSC, vol. 20, no. 5, 2023.
[8] M. Sewak et al., "Deep RL for automated IDS response selection," Computers & Security, vol. 127, 2024.
[9] Y. Lu et al., "PBFT-based IoT data integrity framework," IEEE Access, vol. 11, 2023.
[10] L. Lao et al., "PBFT for edge computing resource management," Future Generation Computer Systems, vol. 150, 2024.
[11] N. Koroniotis et al., "Towards the development of realistic botnet dataset: BoT-IoT," FGCS, vol. 100, 2019.
[12] R. Sutton and A. Barto, Reinforcement Learning: An Introduction, MIT Press, 2018.
[13] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," OSDI, 1999.
[14] T. Li et al., "Federated learning: Challenges, methods, and future directions," IEEE SPM, vol. 37, no. 3, 2020.
[15] Syed Faraz Afsar, "CYBERSECURITY FRAMEWORK FOR SECURE CLOUD COMPUTING USING BLOCKCHAIN AND FEDERATED DEEP LEARNING", PRJ, vol. 4, no. 6, pp. 280–301, Jun. 2026.

[16] Ahmed Wali Khan, "AN AI-DRIVEN BLOCKCHAIN-BASED CYBERSECURITY FRAMEWORK FOR SECURE CLOUD COMPUTING ENVIRONMENTS", SES, vol. 4, no. 6, pp. 1745–1762, Jun. 2026.

[17] L. Zhao, X. Chen, and Y. Li, "Smart contract-based adaptive access control for secure cloud infrastructures," IEEE Transactions on Cloud Computing, 2024.

[18] Wahab, Abdul, et al. "AI and Machine Learning-Driven Framework for Early Detection and Prevention of Ransomware Attacks in Banking Systems."Policy Research Journal (PRJ)3.10 (2025): 751-764.

[19] Sajid, Zubair, et al. "Robust Real-Time 2D Object Detection Using YOLOv5: Architecture, Training Optimization, and Comparative Evaluation."Spectrum of Engineering Sciences(2025).

[20] Sajid, Zubair, et al. "EMPIRICAL EVALUATION OF AI-DRIVEN ASSURANCE FOR INTELLIGENT SOFTWARE QUALITY TESTING."

[21] Abbasi, Muhammad Raheel, et al. "BEHAVIORAL DRIVERS INFLUENCING CLOUD COMPUTING ADOPTION IN PAKISTAN'S FINANCIAL SECTOR: A TPB-BASED EMPIRICAL STUDY."

[22] Mirjat, Tahir Hussain, et al. "Automated Assessment and Learning Framework for Competency-Based Training in TEVT Institutions of Sindh, Pakistan."Spectrum of Engineering Sciences(2025): 1595-1616.

[23] Qureshi, Asif Khalid, et al. "HYBRID SEMI SUPERVISED MULTIMODAL YOLO11 FRAMEWORK FOR ROBUST SOLAR PHOTOVOLTAIC PANEL DEFECT DETECTION."Spectrum of Engineering Sciences4.5 (2026): 760-794.[34] Brohi, Ariz Muhammad, et al. "An Adaptive Sensor Data Access Framework for Mobile and Web Environments."Journal of Information Communication Technologies and Robotic Applications17.1 (2026).

[24] Zheng, Xiao, etal. "Adaptive DNN Partitioning Strategy for Optimized User Fitness in Edge Computing Networks."IEEE Transactions on Consumer Electronics(2026).

[25] Ahmed, E., Ahmed, M., Qureshi, A. K., & Tahir, M. (2026). ADVERSARIALLY ROBUST AND REAL-TIME EXPLAINABLE DETECTION OF CROSS-SITE SCRIPTING ATTACKS By USING ADAPTIVE MACHINE LEARNING.Spectrum of Engineering Sciences,4(1), 754-766.

[26] Qasim, Ghulam, et al. "CONTEXT-AWARE AND EXPLAINABLE HYBRID CLASSIFICATION OF CROSS-SITE SCRIPTING ATTACKS USINGMACHINE LEARNING."Spectrum of Engineering Sciences4.1 (2026): 711-727.

[27] Hou, Mingliang, et al. "Dynamic Graph Learning for Bus Passenger Profiling in Urban Transportation Networks."IEEE Transactions on Intelligent Transportation Systems(2026).

[28] Shah, Imdad Ali, et al. "A FAULT-TOLERANT ADAPTIVE CRYPTOGRAPHIC FRAMEWORK FOR RELIABLE COMMUNICATION IN HYBRID QUANTUM-CLASSICAL ENVIRONMENTS."Spectrum of Engineering Sciences3.12 (2025): 715-726.

[29] Jawaid, Nasreen, et al. "Dimensions of Knowledge Graph Reasoning."Spectrum of Engineering Sciences(2025): 1404-1432.

[30] Zheng, Xiao, et al. "Computation offloading based on incomplete information in edge computing networks."Cluster Computing28.14 (2025): 908.

[31] Bux, Hussain, et al. "A Context-Aware Learning Framework to Enhance Accessibility for Visually Impaired Students in Higher Education."Spectrum of Engineering Sciences(2025).