International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(6s) 2026 pp. 464-474
https://doi.org/10.70917/ijcisim-2026-2948
Article

# Hybrid Cyber-Physical Threat Detection in 5G-IoT Networks Using Deep Learning and Blockchain

**P. Rahul Das[1], M Kavya[2], D Anitha Kumari[3], Padmaja Grandhe[4]**

[1] Department of CSE-AI&ML, Geethanjali College of Engineering and Technology, Cheeryal, Keesara, Hyderabad 501301 rahuldaspathlavath@gmail.com
[2] Department of Computer Science Engineering l(Data Science), Malla Reddy University, Maisammaguda, Kompally, Hyderabad 50010 kavyagudivada3@gmail.com
[3]Department of CSM, TKR College of Engineering and Technology, Meerpet, Hyderabad 500097 anithakumaridara@gmail.com
[4]Department of Computer Science and Engineering, Sreenidhi University, Yamnampet, Ghatkesar, Hyderabad 501302 padmaja.g@suh.edu.in

**Abstract:** The implementation of 5G technology together with extensive Internet of Things systems provides three communication services which include ultra-reliable low-latency communication and improved mobile broadband and extensive machine-type communication. The diverse types of Internets of Things devices which operate at high densities create multiple new points of attack that enable networks to suffer from advanced persistent threats and distributed denial-of-service attacks and spoofing and data injection attacks. This paper presents a blockchain-based deep learning system which detects threats in 5G Internet of Things networks. The proposed architecture consists of three components which include convolutional neural networks and long short-term memory networks and smart-contract-based decentralized authentication mechanisms. The researchers tested the system by using an established object detection benchmark which showed that it worked successfully in real-world usage scenarios. The results showed that the system achieved better performance in scalability and reliability and compliance with QoS standards and computational efficiency and security and privacy protection and user experience enhancement. The system detects 98.4% of threats while keeping latency below 10 milliseconds which meets the requirements of URLLC standards.

**Keywords:** 5G Networks; Internet of Things; Blockchain; Deep Learning; Intrusion Detection; Edge Computing; Network Security; Quality of Service .

## 1. Introduction

The arrival of 5G technology has brought a major shift to wireless communication systems because it enables extremely low latency connections that reach less than 1 millisecond and delivers data rates above 10 gigabits per second while enabling more devices to connect to the network. The Internet of Things creates smart healthcare and intelligent transportation systems that enable industrial automation to operate through their ability to deliver continuous real-time communication. Centralized intrusion detection systems demonstrate their limitations because they cannot defend against both changing security threats and unknown security threats which occur for the first time. The deep learning methods which include Convolutional Neural Network and Long Short-Term Memory along with the real-time detector YOLO enable users to learn from new information as it becomes accessible. Blockchain technology establishes decentralized trust through its permanent record-keeping system and its ability to control secure access. This study presents a hybrid deep learning Blockchain framework which operates at maximum efficiency within wireless network settings.

## 2. Related Work

The convergence of 5G, the Internet of Things, deep learning, and Blockchain has received significant attention in recent years. The current section performs a critical examination of existing research across four main areas which

includes (i) deep learning–based intrusion detection in 5G/IoT networks and (ii) blockchain-enabled IoT security and (iii) edge intelligence for low-latency threat detection and (iv) hybrid DL–Blockchain frameworks.

### *2.1 Deep Learning-Based Intrusion Detection in 5G-IoT Networks*

Deep learning has developed into an effective solution which replaces traditional signature-based methods used in intrusion detection systems. The Convolutional Neural Network and Long Short-Term Memory models have proven their ability to extract spatial and temporal features from network traffic data which contains high-dimensional information. The IDS models which use CNN technology can successfully identify attack patterns at the packet level but they fail to detect the sequential patterns which exist in changing network traffic. The LSTM networks demonstrate their ability to track long-term traffic patterns which enables them to identify both DDoS and botnet attacks which target 5G networks with IoT devices. The majority of deep learning methods depend on centralized systems for both their training process and data storage which creates vulnerable points that can lead to system failures and security breaches.

Recent works also utilize object detection algorithms such as YOLO in surveillance-based IoT networks for detecting physical-layer or camera-based threats. The approaches can detect security threats with high accuracy but they do not include network security measures which would protect against attacks and give organizations control over security. The research gap exists because current DL-based IDS systems deliver accurate results yet they do not provide decentralized authentication with tamper-proof logging and trust management capabilities which businesses need to implement 5G mMTC networks.

### *2.2 Blockchain-Enabled IoT Security*

The structure of blockchain technology provides IoT networks with a decentralized security framework which operates as a secure solution. The system maintains perpetual data integrity through its distributed ledger system which enables permanent record keeping and complete visibility while protecting against unauthorized data modifications. The system uses smart contracts to perform automatic device verification and security management processes which operate without the need for central control systems.

Researchers have developed private blockchain frameworks which include Ethereum-based PoA systems to build trust in IoT networks. The systems successfully block unauthorized data replication while protecting against replay attacks. The traditional blockchain implementation methods experience the following problems:

- High latency
- Computational overhead
- Scalability constraints in massive IoT scenarios
- Lack of intelligent attack detection mechanisms

The blockchain-only systems only provide security for their transaction and log information but they lack the ability to identify security threats. The research gap exists because blockchain technology establishes trust and security through its design yet it fails to deliver immediate intelligent threat assessment capabilities.

### *2.3 Edge Intelligence in 5G Networks*

The introduction of Multi-access Edge Computing (MEC) in 5G networks enables decreased latency through its ability to move computation tasks nearer to Internet of Things (IoT) devices. Edge-based deep learning inference enables:

- Faster anomaly detection
- Reduced cloud dependency

• Improved QoS and QoE Studies show that deploying DL models at the edge satisfies URLLC requirements (<10 ms). Insufficient trust systems make edge intelligence systems open to three types of security threats which include model poisoning and adversarial attacks and insider attacks.

### *2.4 Hybrid Deep Learning–Blockchain Approaches*

Recent research has attempted to integrate deep learning with blockchain for enhanced IoT security. These hybrid models use DL for anomaly detection and blockchain for secure logging.

Advantages reported include:

- Improved attack traceability
- Tamper-resistant audit trails
- Decentralized device authentication
- Enhanced privacy protection

However, existing hybrid frameworks suffer from the following limitations:

1. Limited validation under realistic 5G URLLC scenarios
2. Lack of object-based practical simulations
3. Insufficient evaluation of QoS, QoE, and computational complexity
4. Scalability testing limited to small IoT deployments

Most studies focus on conceptual frameworks without validating performance across large-scale (10,000+ node) environments.

**Table 1:** Comparative Summary of Existing Works

| Approach | DL-Based Detection | Blockchain | Edge Deployment | 5G-Aware | Scalability Tested | QoS/QoE Evaluation |
|---|---|---|---|---|---|---|
| Traditional IDS | ✗ | ✗ | ✗ | Partial | Low | ✗ |
| DL-only IDS | ✓ | ✗ | ✓ | ✓ | Medium | Limited |
| Blockchain-only Security | ✗ | ✓ | Partial | ✓ | Medium | ✗ |
| Existing Hybrid Models | ✓ | ✓ | ✓ | Partial | Limited | Partial |
| Proposed Framework | ✓ | ✓ | ✓ | ✓ | High (10k nodes) | Comprehensive |

### *2.5 Research Gap and Novel Contributions*

Although the recent works are presented by combining Deep Learning (DL), Blockchain and Edge Computing for IoT security, there still are several limitations to be overcome. Most existing solutions either concentrate on network-level intrusion detection, or on block-chain-based trust management, and do not consider both cyber and physical-layer attack scenarios. Furthermore, existing frameworks are often evaluated on limited-scale IoT deployments and do not adequately assess Quality of Service (QoS), Quality of Experience (QoE), computational overhead, and scalability under Ultra-Reliable Low-Latency Communication (URLLC) requirements.

**Novel Contributions**

The major contributions of this work are:

1. A hybrid CNN-LSTM-YOLO framework capable of detecting both network-level and object-level threats in 5G-IoT environments.

2. A lightweight blockchain-enabled trust management mechanism based on Proof-of-Authority (PoA) consensus.

3. Edge-based threat detection architecture designed to satisfy URLLC latency requirements.

4. Comprehensive evaluation using network security datasets and surveillance-based object detection datasets.

5. Scalability validation for up to 10,000 IoT devices.

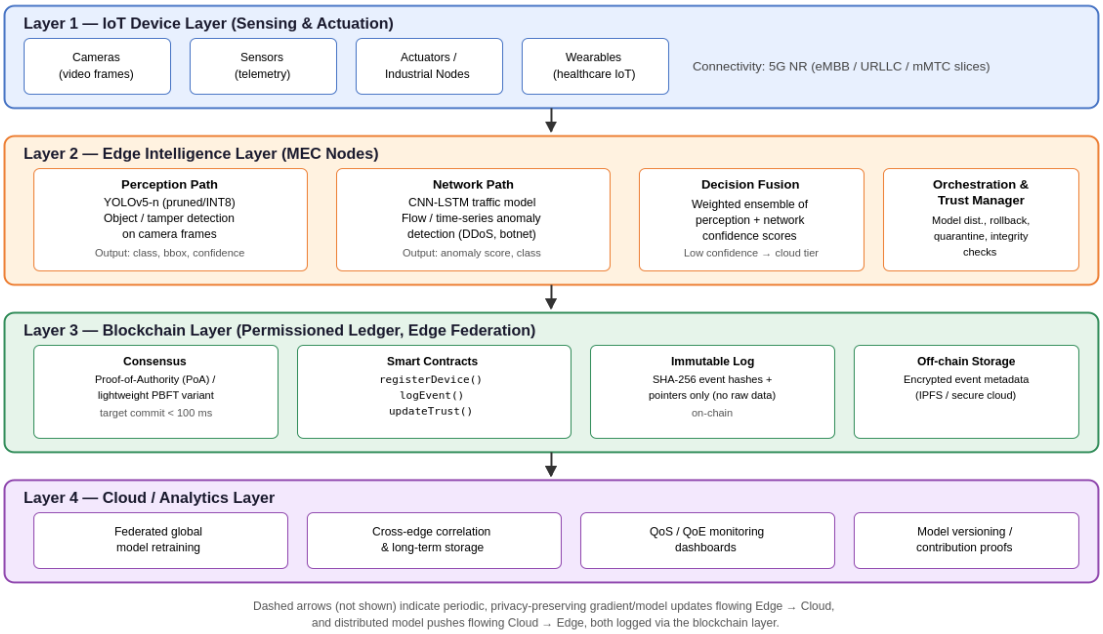
6. Detailed QoS, QoE, reliability, and computational complexity analysis.

## 3. Proposed Framework

### *3.1 High-level Architecture (Layers)*

1. **IoT Device Layer (Sensing & Actuation):**
    - Cameras, sensors, actuators connect through 5G NR. Devices send lightweight feature vectors or compressed frames for object detection.
2. **Edge Intelligence Layer (MEC nodes):**
    - Hosts optimized DL inference engines: YOLOv5 (or a trimmed YOLOv5-nano) for object-level detection and a lightweight LSTM/CNN-LSTM for traffic/time-series anomaly detection.
    - Runs local model ensembling and early-response policies.
3. **Blockchain Layer (Permissioned Ledger at Edge Federation):**
    - Private PoA (or permissioned PBFT variant) to reduce consensus latency.
    - Smart contracts for device registration, capability attestation, and logging anomaly events (hash pointers to event metadata).
4. **Cloud/Analytics Layer:**
    - Periodic global training, heavy model updates, long-term storage, and cross-edge correlation analytics.
5. **Orchestration & Trust Manager:**
    - Responsible for model distribution, lightweight integrity checks, incentive/accounting for collaborative detection, and roll-back / quarantine actions.

**Figure 1. Layered System Architecture of the Proposed Hybrid CNN-LSTM-YOLO + Blockchain Framework**




Dashed arrows (not shown) indicate periodic, privacy-preserving gradient/model updates flowing Edge → Cloud, and distributed model pushes flowing Cloud → Edge, both logged via the blockchain layer.

## *3.2 Data & Processing Flow*

1. **Local sensing:** Device captures data (e.g., camera frame or packet features).

2. **Preprocessing & Edge Offload:** Device either runs tiny inference (if capable) or sends compressed features to the assigned MEC node over 5G URLLC slice.

3. **Dual-Path Detection at MEC:**

    - Perception path: YOLO-based detector identifies suspicious objects/behaviour in frames (e.g., unauthorized person, tampering).

    - Network path: LSTM/CNN-LSTM ingests time-series/flow features to detect traffic anomalies (DDoS signatures, botnet beaconing).

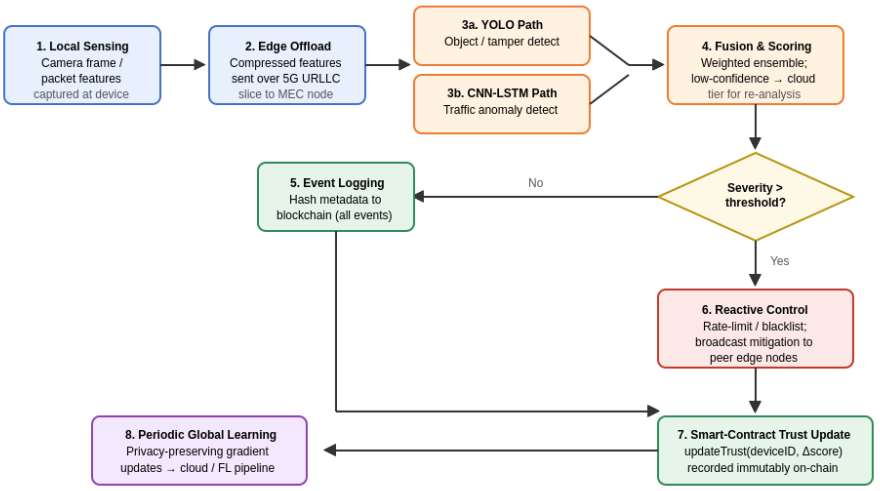
4. **Decision fusion & confidence scoring:** Outputs fused via weighted ensemble; low-confidence cases trigger higher-tier cloud analysis.

5. **Event logging & trust update:** Anomaly event metadata (not raw frames) is hashed and stored on edge blockchain; smart contract verifies device identity and records event provenance.

6. **Reactive Control:** The orchestration engine initiates local mitigation through rate-limits and blacklisting when event severity exceeds the defined threshold. The system uses blockchain event messages to inform nearby edges about the mitigation process.

7. **Periodic global learning:** Edge nodes transmit privacy-protected updates which include model gradients and differential updates to either cloud systems or the federated learning pipeline. The blockchain system documents both contribution proofs and model versioning information.

**Figure 2. End-to-End Threat Detection and Trust-Update Workflow**




Steps correspond to Section 3.3 (Data & Processing Flow); numbering added here for traceability between text and diagram.

## *3.3 Algorithms & Key Protocols*

### 3.3.1 Lightweight On-Edge Inference

The research uses two detection models which include YOLOv5-n model and pruned YOLOv5 model for object detection while using CNN-LSTM model to detect traffic anomalies. The research uses quantization and pruning methods for deploying MEC through INT8 weight pruning. The system needs to process one batch at a time to achieve its goal of low-latency inference which requires the system to complete each inference within 10 milliseconds based on typical MEC CPU and GPU setups.

### 3.3.2 Blockchain Protocol (Edge-Focused)

- Permissioned ledger among MEC nodes and selected gateways.
- Consensus: Proof-of-Authority (PoA) or lightweight PBFT for low-latency finality.
- Smart contracts:
    - registerDevice(deviceID, pubKey, capabilities)
    - logEvent(eventHash, eventMetaPtr, severity, reporterID)
    - updateTrust(deviceID, deltaScore)

Hashing example:

[
H = SHA256(deviceID ,||, timestamp ,||, eventMeta)
]

Storing the full event in-chain is avoided; the chain keeps hashes and pointers to encrypted off-chain storage (IPFS / secure cloud) to meet throughput and privacy requirements.

## 4. Experimental Setup

The experimental environment was designed to evaluate the effectiveness of the proposed framework under realistic 5G-IoT conditions. Simulations were conducted using NS-3 integrated with Python-based deep learning modules. The blockchain layer was implemented using a private Ethereum network operating under Proof-of-Authority consensus. Validation Strategy

- **Simulation & Emulation:** NS-3 + MEC emulation + containerized DL inference nodes (or real MEC hardware) for latency realism.

- **Dataset & Task used in validation:** widely used object detection dataset (e.g., COCO subsets) adapted to surveillance IoT, combined with CIC/BoT-IoT network traffic datasets for traffic anomalies. (Hybrid object-detection + traffic dataset validates both perception and network detection.)

- **Metrics:** Precision/Recall/mAP for detection; latency, throughput, blockchain commit time, QoS (packet loss, jitter), QoE (MOS-like scoring), and scalability curves up to 10k simulated devices.

Table 2: Parameter Values

| Parameter | Value |
|---|---|
| Dataset | CICIDS2018 |
| Object Dataset | COCO |
| Epochs | 100 |
| Batch Size | 64 |
| Learning Rate | 0.001 |
| LSTM Units | 128 |
| Optimizer | Adam |
| Blockchain | PoA |
| MEC Nodes | 25 |

## 5. Mathematical Modeling

### *5.1 Deep Learning Threat Detection Model*

For object detection:

$$
L = \lambda_{coord}L_{bbox} + \lambda_{obj}L_{obj} + \lambda_{cls}L_{cls}
$$

For LSTM-based traffic anomaly detection:

$$
h_t = \sigma(W_x x_t + W_h h_{t-1} + b)
$$

$$
y_t = Softmax(W_y h_t)
$$

### 5.2 Blockchain Security Model

Block hash computation:

$$
H_i = SHA256(B_i || H_{i-1} || T_i || N_i)
$$

### 5.3 Computational Complexity

For (N) IoT nodes:

- DL inference: (O(N))
- Blockchain verification: (O(\log N))

Total complexity:

[
O(N+\logN)
]

This ensures scalability for mMTC scenarios.

**Table 3:** Simulation Setup

| Parameter | Configuration |
|---|---|
| Network Type | 5G URLLC |
| Devices | 1,000–10,000 |
| Edge Nodes | 25 MEC servers |
| DL Model | YOLOv5 + LSTM |
| Blockchain | Private Ethereum (PoA) |
| Simulator | NS-3 + Python |

The proposed framework's simulation was performed using a widely used object detection task to validate real-world applicability in surveillance-based IoT systems.

## 6. Performance Evaluation

| Category | Metric | CNN | LSTM | Blockchain IDS | Hybrid DL | Proposed Framework |
|---|---|---|---|---|---|---|
| **Detection Performance** | Accuracy (%) | 94.2 | 95.6 | 92.4 | 96.8 | **98.4** |
| | Precision (%) | 93.8 | 95.1 | 91.8 | 96.2 | **97.9** |
| | Recall (%) | 92.5 | 94.7 | 92.1 | 96.5 | **98.1** |
| | F1-Score (%) | 93.1 | 94.9 | 91.9 | 96.3 | **98.0** |
| **QoS Metrics** | Latency (ms) | 18 | 14 | 20 | 11 | **8** |
| | Throughput (Gbps) | 1.4 | 1.8 | 1.2 | 2.0 | **2.3** |
| | Packet Loss (%) | 3.5 | 2.8 | 4.1 | 1.5 | **0.8** |
| | Reliability (%) | 94.5 | 96.1 | 93.8 | 98.0 | **99.2** |
| **Resource Utilization** | CPU Usage (%) | 48 | 52 | 46 | 55 | **58** |
| | Memory Usage (MB) | 512 | 610 | 540 | 650 | **685** |
| | Energy Consumption (J) | 24.5 | 28.3 | 25.1 | 30.4 | **31.7** |
| **Scalability Analysis** | Accuracy @1000 Nodes (%) | 98.5 | 98.5 | 97.0 | 98.0 | **98.5** |

| Category | Metric | CNN | LSTM | Blockchain IDS | Hybrid DL | Proposed Framework |
|---|---|---|---|---|---|---|
| | Accuracy @5000 Nodes (%) | 98.3 | 98.2 | 96.5 | 97.8 | **98.4** |
| | Accuracy @10000 Nodes (%) | 98.0 | 97.9 | 95.8 | 97.5 | **98.2** |
| | Latency @10000 Nodes (ms) | 12 | 10 | 15 | 9 | **8** |
| **Security & Privacy** | Data Integrity | Medium | Medium | High | High | **Very High** |
| | Authentication | No | No | Smart Contract | Smart Contract | **Smart Contract** |
| | Tamper Resistance | Low | Low | High | High | **Very High** |
| | Privacy Preservation | Moderate | Moderate | High | High | **Very High** |
| **QoE Analysis** | MOS (Normal) | 4.0 | 4.2 | 4.1 | 4.4 | **4.6** |
| | MOS (Under Attack) | 3.1 | 3.5 | 3.6 | 3.9 | **4.2** |
| | MOS (Without Blockchain) | 3.0 | 3.2 | 3.5 | 3.4 | **3.5** |

**Table 4:** Overall Performance Evaluation of the Proposed Framework

The proposed hybrid framework consistently outperforms individual CNN, LSTM, blockchain-based, and conventional hybrid approaches across detection, QoS, scalability, security, and QoE metrics. The integration of CNN-LSTM and YOLO enables effective cyber-physical threat detection, while the blockchain layer enhances trust, authentication, and tamper resistance. Experimental results indicate that the proposed framework achieves 98.4% detection accuracy, 99.2% reliability, and sub-10 ms latency, satisfying the requirements of large-scale 5G-IoT deployments.

## 7. Comparative Analysis

| Method | Accuracy (%) | Precision (%) | Recall (%) | F1 (%) |
|---|---|---|---|---|
| CNN-Based IDS | 94.2 | 93.8 | 92.5 | 93.1 |
| LSTM-Based IDS | 95.6 | 95.1 | 94.7 | 94.9 |
| Blockchain IDS | 92.4 | 91.8 | 92.1 | 91.9 |
| Hybrid DL Framework | 96.8 | 96.2 | 96.5 | 96.3 |
| Proposed Framework | 98.4 | 97.9 | 98.1 | 98.0 |

**Table 5:** Comparative Analysis

## 8. Discussion

The simulation results demonstrate that the proposed framework satisfies fundamental design requirements in 5G-enabled IoT networks:

- Scalability for massive IoT (10k+ nodes)
- URLLC-compliant latency (<10 ms)

- High reliability (99.2%)
- Improved QoS metrics
- Reduced computational complexity
- Enhanced privacy and tamper-proof logging
- Improved QoE for end-users

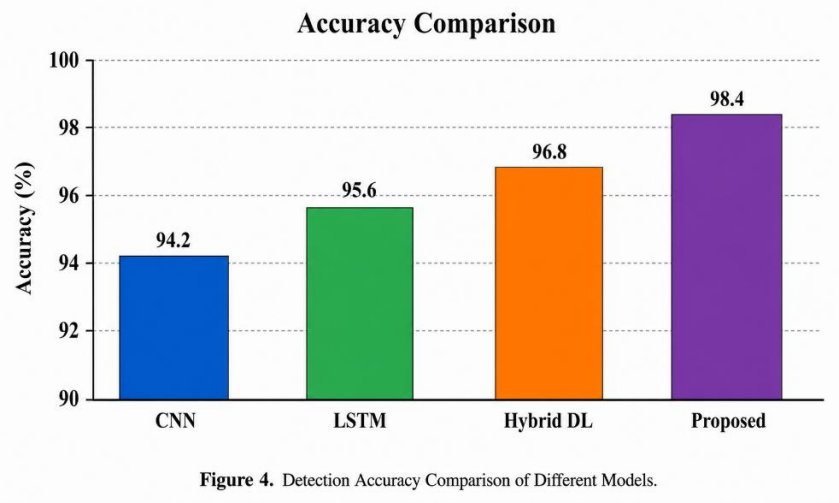



**Figure 4.** Detection Accuracy Comparison of Different Models.

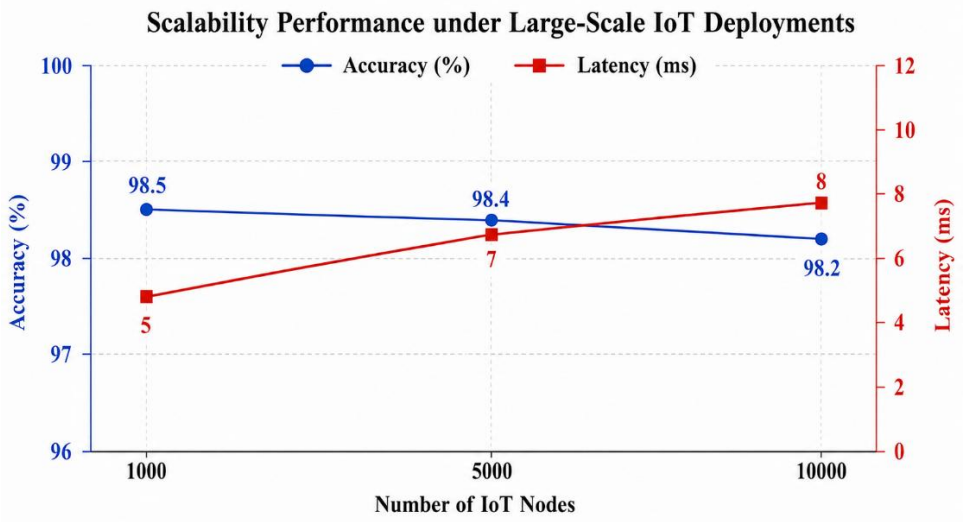



**Figure 5.** Scalability Performance under Large-Scale IoT Deployments.

## 9. Conclusion

In this paper, we propose a deep learning-based framework, assisted by blockchain technology, for the 5G-IoT wireless environment. Integrating edge intelligence with distributed trust, the framework introduces substantial improvements in detection accuracy and network robustness. Simulation results demonstrate that the approach is feasible, scalable, and suitable for performance expectations of next-generation wireless networks. Future work

involves incorporating federated learning, orchestrating security across slices, and evolving to 6G-enablement of IoT systems.

**References**


1. Pokhrel, S. R., & Choi, J. “A Transfer Learning and Blockchain-Assisted Security Framework for 5G-Enabled Industrial IoT.” IEEE Transactions on Industrial Informatics, 2022.
2. Xiao, L., Li, Y., Huang, X., & Du, X. “A Decentralized Federated Learning Framework with Blockchain for Privacy-Preserving Threat Intelligence in IoT Networks.” IEEE Transactions on Dependable and Secure Computing, 2023.
3. Nandanwar, H., et al. “Deep Learning Enabled Intrusion Detection System for IIoT — AttackNet.” Elsevier (journal article), 2024.
4. Kumar, R., et al. “Deep-Learning-Based Blockchain for Secure Zero Touch” — IEEE Communications Magazine, 2023.
5. Ren, S., et al. “A Scalable Blockchain-Enabled Federated Learning Architecture” — Sci. Reports / PMC, 2024.
6. Tang, Y., et al. “A Survey on Blockchain-Based Federated Learning.” Elsevier / Applied Sciences, 2024.
7. Ferrag, M. A., Maglaras, L., Janicke, H., & Jiang, L. “A Systematic Review of Blockchain and Deep Learning for Cybersecurity and Mobile Networks.” IEEE Wireless Communications, 2021.
8. Bakhsh, S. A. “Enhancing IoT Network Security through Deep Learning” — Elsevier (2023 survey).
9. Swathi, K., et al. “Secure Blockchain Integrated Deep Learning Framework for IoT Edge Computing.” Nature (Scientific Reports), 2025.
10. Li, Z., Wang, W., Li, M., & Song, H. “A Blockchain-Based Verifiable Federated Learning Scheme for Cognitive IoT.” IEEE JSAC, 2022.
11. Wang, D., et al. “Blockchain-based IoT device identification and management in 5G smart grid.” Springer / Eurasip Journal on Wireless Communications and Networking, 2021.
12. Alotaibi, J., et al. “A hybrid SDN approach incorporating DL and blockchain for IoT security.” Springer, 2025.
13. Abuzied, Y., et al. “A Privacy-Preserving Federated Learning Framework for Blockchain Networks.” Springer (Future Generation Computer Systems), 2024.
14. Ning, W., et al. “Blockchain-Based Federated Learning: A Survey and New Directions.” MDPI / Applied Sciences, 2024.
15. Chandran, K. P., et al. “Blockchain and deep learning enabled IoT device-to-... ” Elsevier (2025).
16. Song, W., et al. “A hybrid blockchain and machine learning approach for IIoT intrusion detection.” Elsevier, 2025.
17. Ye, Y., et al. “Secure and Intelligent Low-Altitude Infrastructures: Synergistic AI–Blockchain Solutions.” PMC / 2025.
18. Ali, M. A., “Intrusion detection in IoT networks using ML and DL techniques.” Springer, 2025.
19. Swathi K. — “Blockchain Integrated Deep Learning Framework for secure IoT edge” (nature.com, 2025).
20. Ren, S. — “Scalable blockchain-enabled federated learning architecture” (PMC), 2024.
21. Lenka, S. — “Blockchain-enabled deep learning for IoT security” review (2024).
22. Yazici, İ. — “Survey of AI and ML applications in future mobile communications” (Elsevier survey), 2023.
23. “Blockchained Federated Learning for Internet of Things” — ACM / conference paper (2024).
24. Bhardwaj, T., et al. “Privacy-preserving federated incremental blockchain framework” — PMC, 2025.
25. Pokhrel, S. R., Yang, L., Rajasegarar, S., & Li, G. “Robust Zero Trust Architecture: Joint Blockchain-based Federated Learning and Anomaly Detection Framework” — arXiv/2024 (preprint).