Computational Engineering and Technology Innovations

www.ceti.reapress.com

Comput. Eng. Technol. Innov. Vol. 2, No. 2 (2025) 99–106.

Paper Type: Original Article

Enhancing QoS in Computer Networks Through IoT Integration

Nadia Ghasemabadi[1], Omar Mar Cornelio[2,*], Haoran Yu[3]

[1] Department of Computer Engineering, Ayandegan University, Tonkabon, Iran; ghasemabadinadia@gmail.com.

[2] Centro de Estudio de Matematica Computacional, Universidad de las Ciencias Inform aticas, La Habana, Cuba; omarmarcornelio@gmail.com.

[3] School of Economics and Management, China Three Gorges University, China.

Citation:

Received: 12 November 2024 *Revised: 10 January 2025* *Accepted: 22 April 2025*	Ghasemabadi, N., Cornelio, O. M., Yu, H. (2025). Enhancing QoS in computer networks through IoT integration. *Computational Engineering and Technology Innovations*, 2(2), 99-106.

Abstract

Integrating Internet of Things (IoT) in computer networks introduces new opportunities and challenges in ensuring Quality of Service (QoS) across increasingly interconnected systems. As IoT devices proliferate, networks must manage large volumes of data while maintaining low latency, optimal bandwidth utilization, and reliable connectivity. Traditional network models struggle to meet these demands, especially in dynamic environments. This paper explores how IoT integration enhances QoS by enabling real-time monitoring, efficient traffic management, and adaptive resource allocation within networks. It highlights the role of intelligent protocols and architectures, including Software-Defined Networking (SDN) and edge computing, to ensure scalability and performance. Furthermore, this research addresses how predictive analytics and IoT-driven automation improve fault tolerance, reduce downtime, and minimize network congestion.

This paper demonstrates, through an analysis of recent studies and practical implementations, that IoT-enhanced networks can significantly optimize QoS across applications such as healthcare, transportation, and industrial automation. The findings suggest that a well-orchestrated integration of IoT not only meets the growing performance demands but also ensures sustainable and secure network management.

Keywords: Internet of thing, Quality of service, Edge computing, Software-defined networking, Network optimization, Real-time monitoring, Adaptive resource management.

1 | Introduction

The rapid expansion of the Internet of Things (IoT) is reshaping modern computer networks by interconnecting a vast array of devices, sensors, and systems. This interconnected ecosystem offers new possibilities for network efficiency, automation, and real-time monitoring. However, integrating IoT into

Corresponding Author: omarmarcornelio@gmail.com

https://doi.org/10.48314/ceti.vi.71

existing networks presents challenges in maintaining Quality of Service (QoS), especially in latency, bandwidth optimization, reliability, and data management [1].

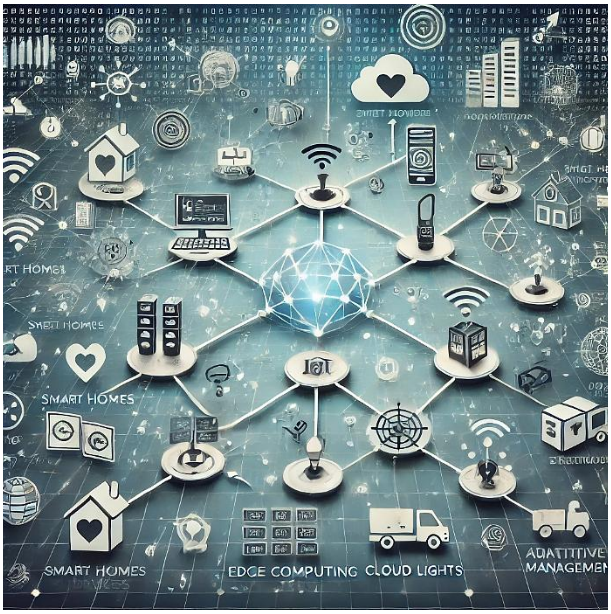

Fig. 1. Conceptual representation of IoT-enhanced computer networks and QoS optimization.

Image showing seamless communication between IoT devices, edge computing nodes, and cloud infrastructure to maintain low latency and efficient resource management [2].

Traditional network architectures struggle to meet the demands of IoT environments due to the massive data exchange between devices, which can overwhelm networks, causing delays and congestion. Maintaining service-level agreements (SLAs) in such dynamic systems becomes increasingly complex as the number of devices grows. Ensuring QoS in these networks is crucial for supporting critical services such as healthcare, industrial automation, and smart infrastructure [3].

Integrating IoT solutions within computer networks introduces new opportunities to enhance QoS. Using technologies like edge computing, Software-Defined Networking (SDN), and Network Function Virtualization (NFV), data can be processed closer to its source, reducing latency and improving responsiveness. This reduces dependence on centralized cloud servers, optimizes bandwidth, and lowers the risk of bottlenecks [4].

Table 1. Integrating IoT solutions.

Challenge	Description
Data management	Handling and processing large volumes of data generated by IoT devices efficiently.
Latency reduction	Ensuring low-latency communication to support time-sensitive applications.
Bandwidth optimization	Managing network traffic to prevent congestion and optimize resource utilization.
Network reliability	Maintaining consistent and reliable network performance, especially in critical scenarios.
Scalability	Ensuring the network can accommodate a growing number of IoT devices seamlessly.
Security and privacy	Protecting sensitive data transmitted and processed within the IoT network.
Heterogeneity	Integrating diverse IoT devices with different protocols and communication standards.
Energy efficiency	Balancing performance and energy consumption, especially in battery-powered devices.
Resource allocation	Dynamically allocating resources based on varying network conditions and demand.
Interoperability	Ensuring smooth communication between IoT systems and legacy infrastructure.
Fault tolerance	Developing mechanisms for network resilience to recover from failures quickly.
Regulatory compliance	Adhering to laws and standards regarding data privacy, cybersecurity, and network use.

2 | Background and Related Work

2.1 | IoT Integration in Modern Networks

IoT-enabled networks consist of interconnected sensors, devices, and systems that generate large volumes of data across multiple domains, including healthcare, industrial automation, transportation, and smart infrastructure. These networks support real-time applications such as remote patient monitoring, predictive maintenance, environmental monitoring, and automated traffic management. To maintain QoS in these environments, networks must ensure low latency, high reliability, optimal bandwidth usage, and dynamic resource allocation.

This section explores how IoT integration affects the network's ability to deliver reliable performance while addressing the challenges posed by massive data generation, device heterogeneity, and dynamic network conditions.

2.2 | Limitations of Traditional Network Architectures

Traditional network architectures, built around centralized data processing in cloud servers, struggle to meet the growing demands of IoT environments. Key limitations include [5]:

I. Latency issues: Critical IoT applications such as healthcare monitoring or industrial control systems require near-instantaneous data processing, but cloud-based systems introduce delays due to centralized data transfer.

II. Bandwidth constraints: Transmitting large volumes of data from distributed IoT devices to the cloud consumes significant bandwidth, creating potential bottlenecks and impairing service quality.

III. Scalability challenges: As the number of IoT devices grows, networks must handle increased data traffic, but traditional architectures are often ill-equipped to manage these surges effectively.

IV. Data privacy concerns: Sensitive data transmitted to cloud servers is vulnerable to breaches, creating security and regulatory compliance concerns.

These challenges necessitate more efficient architectures that bring data processing closer to the source, reducing latency and optimizing network resources [6].

2.3 | Role of Edge Computing in Enhancing QoS

Edge computing addresses many of the limitations of traditional cloud-based architectures by distributing computational tasks closer to the IoT devices, minimizing latency and bandwidth usage. This localized processing improves QoS for time-sensitive applications by enabling faster decision-making and reducing network congestion.

Key use cases include:

I. Smart transportation: Edge computing enables real-time traffic management by analyzing data from sensors, cameras, and traffic signals, optimizing traffic flow and reducing congestion.

II. Healthcare monitoring: Wearable IoT devices monitor patients in real-time, with edge computing providing instant alerts for emergencies, reducing latency compared to cloud-based systems.

III. Industrial automation: In manufacturing, edge computing ensures continuous monitoring and predictive maintenance by processing data locally, preventing equipment failures and downtime.

IV. Smart utilities: IoT-enabled grids use edge computing to balance energy distribution and detect real-time anomalies in water or electricity systems, ensuring efficient resource management.

By offloading tasks to the edge, IoT-integrated networks can guarantee higher QoS with faster responses, reduced bandwidth usage, and improved reliability.

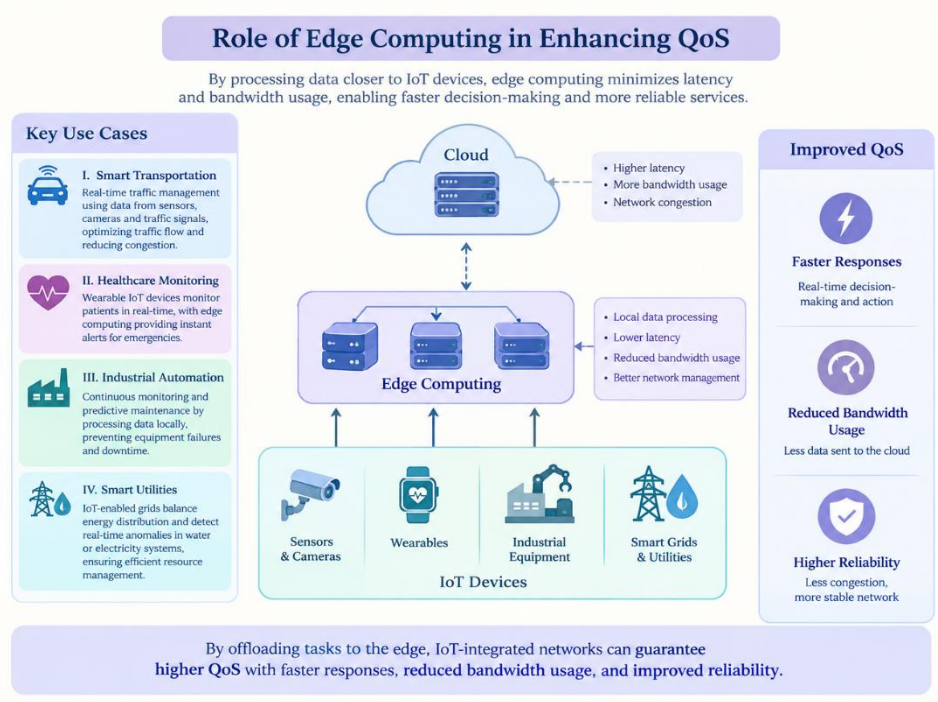

Fig. 1. Role of edge computing in enhancing QoS through IoT integration.

This illustration demonstrates how edge computing reduces latency by processing data locally, optimizes bandwidth, and ensures efficient network management through decentralized IoT-based infrastructure.

2.4 | AI-Driven Optimization in IoT Networks

Integrating Artificial Intelligence (AI) further enhances IoT-based networks by optimizing resource management and improving QoS. AI techniques like machine learning and predictive analytics allow edge nodes to make autonomous decisions, enabling real-time analytics and proactive fault management. Key AI-driven optimizations include:

I. Dynamic resource allocation: AI algorithms monitor network traffic and allocate resources based on real-time demand, preventing congestion and ensuring smooth service delivery.

II. Task offloading: Intelligent task offloading between edge devices and cloud servers optimizes computational efficiency, balancing workload to maintain QoS.

III. Predictive maintenance: AI models analyze data from IoT sensors to predict potential network failures, enabling proactive measures to prevent disruptions.

IV. Federated learning: This distributed AI model allows edge nodes to train machine learning models collaboratively without sharing raw data, improving privacy and security.

Through AI-driven automation, IoT networks enhance QoS and ensure scalable, energy-efficient, and secure operations, meeting the demands of modern applications.

3 | Proposed IoT-Driven Framework for Enhancing QoS in Computer Networks

3.1 | System Architecture

The proposed framework for enhancing QoS in computer networks integrates three main layers: IoT Devices, Edge Nodes, and Cloud Servers. This multi-layered architecture ensures low-latency data processing, optimal resource management, and reliable network performance. IoT devices generate real-time data processing locally at edge nodes using AI models. The cloud servers manage large-scale data analysis, long-term storage, and training of AI models. At the same time, the edge nodes focus on real-time decision-making, ensuring efficient QoS across the network.

3.1.1 | IoT devices layer

IoT devices generate real-time data streams that contribute to efficient network operation. Examples include sensors monitoring network health, devices tracking traffic patterns, and monitoring nodes checking bandwidth usage and latency. These devices have limited computational resources, so they offload the data to nearby edge nodes for processing and optimization.

3.1.2 | Edge layer

The edge layer consists of distributed nodes strategically located near IoT devices. These edge nodes handle local data processing, enabling real-time decision-making and optimization without requiring every data packet to travel to a central cloud server. This reduces network latency and optimizes bandwidth utilization, ensuring higher QoS. AI models deployed at edge nodes facilitate tasks such as:

I. Traffic monitoring to manage network congestion.

II. Bandwidth optimization to prevent bottlenecks.

III. Anomaly detection to ensure service continuity and security.

By offloading processing to the edge, network efficiency improves and minimizes the burden on cloud infrastructure.

3.1.3 | Cloud layer

The cloud layer is critical in data aggregation, long-term storage, and large-scale analysis. It handles computationally intensive tasks such as training AI models and predictive analytics. The edge nodes periodically sync with the cloud to receive updated models and algorithms, ensuring continuous optimization across the network.

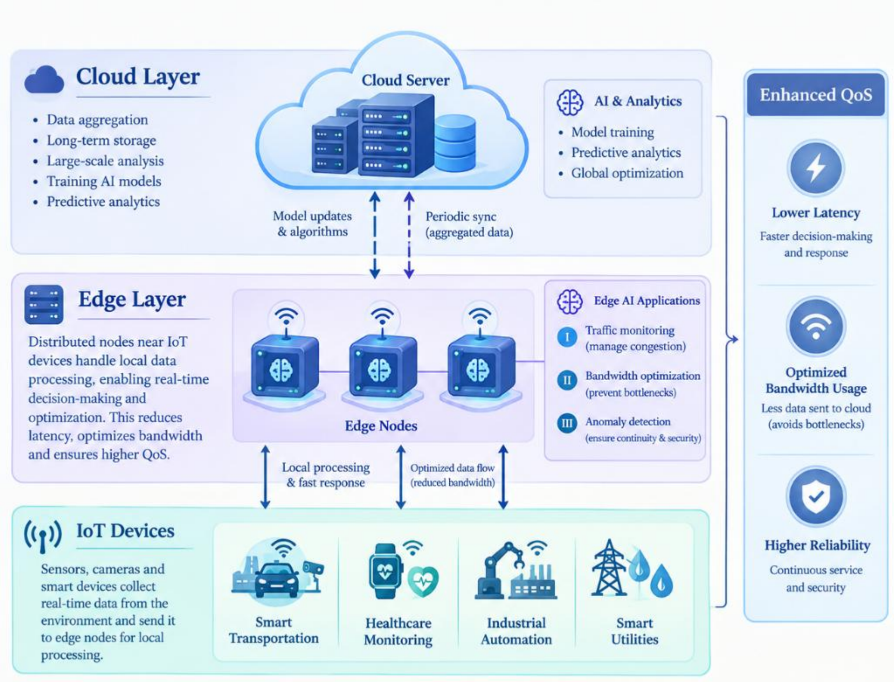

Fig. 2. IoT-driven network architecture for enhanced QoS.

This figure demonstrates the three-layered IoT-driven architecture, where edge computing reduces latency, and the cloud manages large-scale analytics, ensuring efficient QoS.

3.2 | AI Algorithms at the Edge for QoS Enhancement

Integrating AI algorithms at edge nodes brings intelligence to network operations, allowing the system to make dynamic, localized decisions and maintain high QoS. Several AI models are implemented at the edge layer:

3.2.1 | Deep learning

Deep learning models such as Convolutional Neural Networks (CNNs) are deployed for real-time network traffic monitoring. These models allow edge nodes to detect network anomalies and optimize routing dynamically, ensuring consistent QoS.

3.2.2 | Reinforcement learning

Reinforcement Learning (RL) is applied to adaptive resource management. In scenarios like load balancing and bandwidth allocation, RL algorithms help edge nodes learn from traffic patterns and optimize network performance in real time by making dynamic adjustments to resource allocation.

3.2.3 | Federated learning

Federated learning allows edge nodes to collaborate in training AI models without sharing raw data. Each edge node trains a local model and sends only the model updates to the cloud for aggregation, preserving data privacy while reducing network congestion. This decentralized learning approach ensures high performance and compliance with data privacy regulations.

This framework combines IoT, AI, and edge computing to ensure optimal QoS in modern computer networks, meeting the demands of latency-sensitive applications, bandwidth optimization, and dynamic traffic management [7].

4 | Application Scenarios for Enhancing QoS in Computer Networks through IoT Integration

4.1 | Management in Computer Networks

IoT-driven network monitoring ensures optimal traffic flow in data networks by analyzing real-time packet transmission patterns. Edge devices at strategic network points (e.g., routers and switches) autonomously manage congestion control and bandwidth allocation, reducing delays. AI-based traffic optimization ensures smooth network performance by dynamically adjusting traffic signals and load balancing mechanisms for enhanced QoS.

4.2 | Smart Energy Management in Networks

IoT sensors monitor the power consumption of network devices, identifying energy inefficiencies and enabling predictive maintenance. AI models at the edge predict network demand and optimize resource allocation by dynamically adjusting energy usage. This ensures power efficiency while maintaining high QoS, preventing unnecessary downtime, and improving device longevity.

4.3 | Network Health Monitoring and Anomaly Detection

IoT-enabled sensors continuously track the network's health by monitoring latency, jitter, and packet loss. AI-powered edge nodes analyze these metrics to detect anomalies, such as sudden bandwidth spikes or potential Distributed Denial of Service (DDoS) attacks. Immediate detection ensures proactive maintenance and prompt corrective actions, keeping network operations stable and efficient [8].

5 | Performance Evaluation

5.1 | Latency Reduction

The framework ensures real-time responses to critical events by processing data at the network edge. Compared to traditional centralized architectures, this distributed model minimizes round-trip delays, enhancing QoS for latency-sensitive applications like video streaming and online gaming.

5.2 | Bandwidth Optimization

The proposed architecture reduces the amount of data transferred to the cloud by pre-processing traffic at the edge. This ensures efficient bandwidth usage, enabling networks to handle increased traffic loads without compromising QoS. Packet prioritization algorithms running on edge nodes also allocate bandwidth dynamically based on application needs.

5.3 | Scalability

The distributed nature of edge computing facilitates network scalability by allowing new IoT devices and edge nodes to be added without burdening the cloud infrastructure. Localized data processing ensures networks remain responsive even as traffic volume increases, enhancing QoS and operational efficiency [8].

6 | Challenges and Future Directions

6.1 | Security and Privacy

Integrating IoT devices and edge nodes into networks introduces potential vulnerabilities. Data privacy and network security are crucial, especially when sensitive data flows through multiple edge devices. Techniques like encryption and federated learning can help mitigate risks, but further research is needed to ensure robust security frameworks.

6.2 | Resource Constraints

Edge nodes have limited computational and storage capabilities compared to centralized cloud servers. Efficient algorithms for model compression and optimization are essential to deploy AI models that require fewer resources while maintaining high QoS standards.

6.3 | AI Model Updates and Maintenance

Maintaining consistent AI model updates across edge nodes presents a challenge. Although federated learning reduces the need to transfer large datasets, frequent updates are still required to account for changing network conditions. Research on more efficient update mechanisms is essential to enhance QoS in evolving networks [9].

7 | Conclusion

Integrating IoT and AI-driven edge computing significantly enhances QoS in computer networks. By moving computation closer to the source of data generation, edge computing reduces latency and alleviates bandwidth constraints, ensuring seamless network operations. This decentralization of processing power allows networks to respond proactively to traffic spikes and anomalies, preventing service disruptions and ensuring smooth performance.

As IoT sensors continuously monitor network health, AI models at the edge offer real-time solutions to maintain optimal QoS. The ability to dynamically adjust bandwidth and manage congestion ensures efficient resource utilization, even in dense or large-scale networks. Furthermore, federated learning enhances security and privacy by distributing model training across nodes without sharing raw data, supporting compliance with data protection standards.

In the future, the synergy between AI, IoT, and edge computing will shape more resilient and adaptive networks capable of meeting modern challenges. As networks become more complex and traffic-intensive, this integrated framework will ensure that scalability, efficiency, and QoS remain at the forefront of network design and operations [11].

Acknowledgments

I want to express my gratitude to all those who contributed to the successful completion of this research on Enhancing QoS in Computer Networks through IoT Integration.

Additionally, I am grateful to my peers for their insights into AI algorithms and data analysis, which refined key aspects of this work. Lastly, I thank my family and friends for their unwavering support and motivation throughout this journey.

Funding

This research received no external funding.

Data Availability

The data supporting this study are derived from publicly available sources, including academic publications, case studies, and industry reports on IoT integration and QoS optimization.

Conflicts of Interest

The author declares no conflicts of interest concerning the publication of this research.

References

[1] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE internet of things journal*, *1*(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

[2] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021

[3] Xu, L. Da, He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE transactions on industrial informatics*, *10*(4), 2233–2243. https://doi.org/10.1109/TII.2014.2300753

[4] Duan, S., Wang, D., Ren, J., Lyu, F., Zhang, Y., Wu, H., & Shen, X. (2023). Distributed artificial intelligence empowered by end-edge-cloud computing: A survey. *IEEE communications surveys and tutorials*, *25*(1), 591–624. https://doi.org/10.1109/COMST.2022.3218527

[5] Sun, Y., Song, H., Jara, A. J., & Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. *IEEE access*, *4*, 766–773. https://doi.org/10.1109/ACCESS.2016.2529723

[6] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: vision and challenges. *IEEE internet of things journal*, *3*(5), 637–646.https://doi.org/10.1109/JIOT.2016.2579198

[7] Mammen, P. M. (2021). *Federated learning: Opportunities and challenges*. https://arxiv.org/abs/2101.05428

[8] Pratap, A., Nayan, H., Panda, P., & Mohapatra, H. (2024). Emerging technologies and trends in the future of smart cities and IoT: A review. *Journal of network security computer networks*, *10*(2), 28–38. https://matjournals.net/engineering/index.php/JONSCN/article/view/606

[9] Mehmood, M. Y., Oad, A., Abrar, M., Munir, H. M., Hasan, S. F., Muqeet, H. A. U., & Golilarz, N. A. (2021). Edge computing for IoT-enabled smart grid. *Security and communication networks*, *2021*(1), 5524025. https://doi.org/10.1155/2021/5524025

[10] Alvarez-Campana, M., López, G., Vázquez, E., Villagrá, V. A., & Berrocal, J. (2017). Smart CEI moncloa: An iot-based platform for people flow and environmental monitoring on a Smart University Campus. *Sensors*, *17*(12), 2856. https://doi.org/10.3390/s17122856

[11] Dhanraj, T., Kumar, M., Singh, S., Kumar, R., Jaiswal, P., & Mohapatra, H. (2024). A review on mitigating privacy risks in IoT-enabled smart homes. *Computer networks and communications*, *2*(1), 146–163. https://doi.org/10.37256/cnc.2120244736