Journal of Wireless Networks and Communication Systems
Vol. 2, Issue. 2, Apr-Jun 2026, pp. 1~13
ISSN: 3107-6432, DOI: 10.32595/jwncs/v2i2.2026.28

An Energy-Efficient AI-Assisted Quantum-Secure Communication Framework for Scalable and Reliable IoT Networks

R. Madhubala[1], Prashanth Kumar Bolisetty[2]

[1,2]Faculty of Software Engineering and Data Technologies Unit, Department of Computing and Information Sciences, University of Technology and Applied Sciences-Shinas Al Aqr, Shinas, Sultanate of Oman.

E-mail: r.madhubala@utas.edu.om[1], prashanth.bolisetty@utas.edu.om[2]

Article Info

Article History:

Received Mar 19, 2026
Revised Apr 20, 2026
Accepted May 22, 2026

Keywords:

Quantum Key Distribution (QKD),
AI-Assisted Communication,
Internet of Things (IoT),
Energy Efficiency,
Secure Wireless Networks

ABSTRACT

The fast growth of Internet of Things (IoT) networks has heightened the demand for secure, scalable and energy efficient communications methods. Traditional cryptographic techniques are more susceptible to quantum computing attacks and therefore have pushed the necessity for quantum secure methods. This study presents an energy efficient artificial intelligence assisted quantum secure communication framework designed to scale and provide reliable IoT networks. The framework uses Quantum Key Distribution (QKD) combined with deep learning optimization to improve both relationship and network performance.

A self-adaptive AI module applies its lower level of computational resources and dynamically changing network conditions in order to optimize key management, routing decisions, and resource allocation, which reduces both energy consumption and communication latency. The proposed system is intended to support the specific types of constraints faced within an IoT environment. The experimental simulation results demonstrate that the framework improves energy efficiency, increases packet delivery ratio, and decreases latency in IVN (Intelligent Vehicular Networks) by comparison with traditional means of secure communication.

In addition, by combining AI and quantum communications, we increase our resilience to threats posed by both classical and quantum forms of attack while providing an added layer of protection for transmitting data between devices in future wireless networks. Additionally, this proposed framework will provide a very scalable and effective method for providing IoT solutions within the environment of 5G mobile networks or later generations.

Corresponding Author:

R. Madhubala,
Faculty of Software Engineering and Data Technologies Unit, Department of Computing and Information Sciences,
University of Technology and Applied Sciences-Shinas Al Aqr, Shinas, Sultanate of Oman.
E-mail: r.madhubala@utas.edu.om

1. INTRODUCTION

Advancements in IoT (Internet of Things) continue to rapidly transform how we communicate today by ensuring that billions of smart devices in various industries — health care, smart cities, industrial and transportation systems, etc., can seamlessly connect with each other using an ever-increasing number of wireless networks [1,2]. As this exponential growth has taken place, so too has the volume of sensitive information being transmitted over wireless networks and, therefore, increasing concern over data security, privacy, scalability, and energy efficiency. Many of the existing cryptography techniques that have been used to provide protection to IoT communications (e.g., public key encryption, symmetric keys) are now vulnerable to new types of computational threats, especially with the emergence of quantum computing [3,4].

By utilizing the properties of quantum mechanics (superposition and entanglement), quantum communication is a groundbreaking way to create secure communications [5]. Quantum Key Distribution (QKD) is the most popular form of quantum communication and provides theoretically unbreakable security for key exchanges. However, the use of quantum-secure communication in IoT systems will be limited by such factors as lack of resources; complexity; variable structure; and power restrictions [6].

Simultaneously, immense potential exists for utilizing artificial intelligence (AI) and, in particular, deep learning, to improve the performance of wireless communications by allowing for automated decision-making, intelligent resource allocation, and predictive network management [7,8]. AI-driven techniques have the ability to manage the complexity and diversity of IoT (Internet of Things) networks, providing an effective foundation for integration with quantum communications [9]. Furthermore, the combination of quantum communications and AI represents a viable direction for building secure, scalable, and energy-efficient next-generation wireless systems.

In response to the challenges of creating an energy-efficient and AI-assisted Quantum Secure Communication (QSC) framework for IoT networks, this research proposes an innovative combination of Quantum Key Distribution (QKD) and a Deep Learning-based optimization model to create a QSC framework capable of enhancing the security, decreasing energy consumption and increasing performance of large scale IoT networks. Through the use of an adaptive AI module, we will be able to automatically adjust routing protocols, key management, and resource allocation in real time as we deal with new and changing conditions on the network. This framework will also allow us to protect the network from any and all classical and quantum attacks and provide us with important performance metrics such as latency, throughput, and PDR (Packet Delivery Ratio).

This research makes important contributions to the development of quantum communications by creating: (i) a quantum communication framework that uses a combination of hybrid AI techniques for IoT-type environments; (ii) an energy-efficient optimisation function for effectively using resources; (iii) a method for distributing and routing keys that is efficient, secure, and intelligent; and (iv) an evaluation of the performance of all aspects of the implementation, including demonstrating significantly greater energy efficiency compared to conventional techniques, lower latency and an increase in the overall reliability of device communications through the use of quantum technology.

The remaining section of this research paper is structured as follows: Section 2 provides a literature review of the state-of-the-art in quantum communication and artificial intelligence-enhanced Internet of Things (AI-enhanced IoT); Section 3 presents a description of the system design; Section 4 describes the methodology used to develop the algorithm as well as the

algorithmic structure; Section 5 examines results of the simulation and performance evaluation; and Section 6 concludes with future research directions.

2. LITERATURE REVIEW

[10] Suggested a dynamic routing approach for Quantum Key Distribution (QKD) networks utilizing trusted nodes and quantum repeaters. Their approach enhances the efficiency of secure key generation by adjusting routing choices based on prevailing network conditions. The research showed enhanced network efficiency and dependable communication security in quantum-enabled settings.

[11] Created an innovative method utilizing Deep Reinforcement Learning for the determination of routing and resource distribution in QKD Optical Networks. Additionally, this approach employs smart resource allocation and offers more efficient pathways while adapting to the fluctuating network conditions. The findings of their research indicate enhanced scalability and reduced communication resource overhead.

[12] Recommended routing methods that incorporate reliable relay nodes in order to route QKD networks. The goal of the study was to improve successful key relay through dynamically recomputing paths based on the availability of keys and the conditions of the network. This method resulted in a much higher routing success ratio for large quantum networks than before.

[13] Designed a multiuser quantum key distribution (QKD) system using a deep reinforcement learning algorithm (Deep Q-Network (DQN)). The proposed intelligent adaptive routing and trust-based resource management were used in the new framework to increase the efficiency of security communications in dynamic quantum networks.

3. METHODOLOGY

3.1 System Model

The suggested framework embraces a wide-scale IoT network containing many sensor nodes, gateways, and base stations (NN). Sensors are usually limited by their supply of power, their ability to perform calculations, and their ability to hold data. The general operation of the network is also subject to change and require secure and efficient communications. A visual overview of the system proposed is provided in the Figure 1.

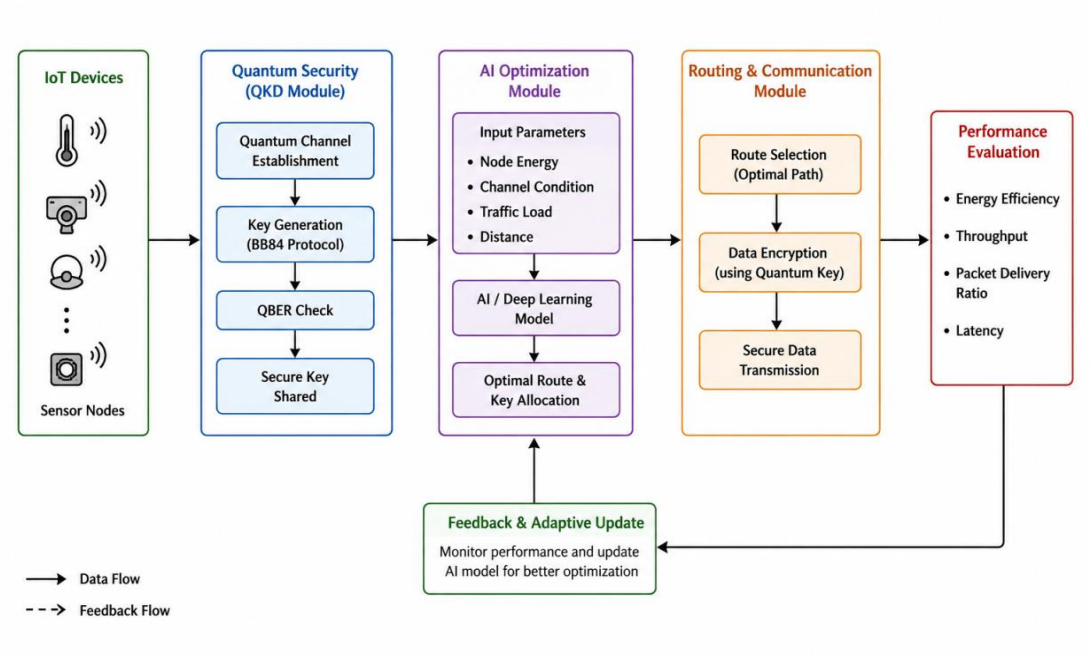

Figure 1. Proposed System Architecture

To tackle these challenges, the suggested system combines three key elements: (i) a Quantum Key Distribution (QKD) module for safe key exchange, (ii) an AI-supported optimization module for smart decision-making, and (iii) a communication layer for data routing and transmission. The main goal is to improve security while reducing energy use and communication lag.

3.2 Quantum Key Distribution Model

The framework uses BB84 QKD protocol for secure communications between nodes. The two nodes will share a secret key generated from quantum states. An eavesdropper attempting to intercept QKD traffic will create a disturbance that will be detectable on the quantum channel.

The secret key generation rate R is expressed as:

$$R = Q[1 - H(e)] \qquad (1)$$

where Q symbolizes the transmission rate of quantum bits and e indicates the quantum bit error rate (QBER). The function (e) refers to the binary entropy function, which is defined as:

$$H(e) = -e\log_2(e) - (1-e)\log_2(1-e) \qquad (2)$$

This equation shows that the effective key generation rate decreases with increasing error rate (due to noise or attacks). Therefore, it is important to keep the QBER low for efficient and secure communication.

3.3 Energy Consumption Model

In IoT networks, energy efficiency is extremely important because the battery capacity of sensor nodes is limited. The total energy consumption of the network is expressed as the sum of the transmission, reception, and processing energy of all nodes in the network:

$$E_{Total} = \sum_{i=1}^{N} \left(E_{tx,i} + E_{rx,i} + E_{proc,i}\right) \qquad (3)$$

Here, $E_{tx,i}, E_{rx,i}$, and $E_{proc,i}$ represent the energy consumed by node i during transmission, reception, and processing, respectively.

The energy required for transmission relies on both the power of transmission and the length of time, expressed as:

$$E_{tx} = P_t \times t \qquad (4)$$

This approach aids in measuring energy consumption and allows the AI model to identify energy-saving communication routes.

3.4 AI-Based Optimization Model

The use of an AI-based deep learning model included in the Framework for optimizing network performance by predicting optimum routes and resource allocation from previously trained data of network conditions. This model is fed with node residual power, channel condition, distance from the node, and amount of traffic as input features. The neural network specifies how the features are processed through the nodes in the Neural Network:

$$y = f(W_x + b) \qquad (5)$$

where x is the input vector, W and b are trainable parameters, and $f(.)$ is a nonlinear activation function. The output y represents the optimal decision (e.g., route selection).

A composite loss function is established to steer the learning process:

$$L = \alpha E_{Total} + \beta D + \gamma(1 - PDR) \qquad (6)$$

The loss function is specifically defined to minimize E_{Total}, D and maximize PDR (thereby minimizing packet loss). The weighting factors (α, β, γ) define the relative importance of each metric.

3.5 Secure Routing Mechanism

In addition to using machine learning to inform about expected routing conditions, additional real-time routing conditions are used to influence routing decisions. A routing metric, denoted as M, is used to evaluate the capability of each node to forward data:

$$M = \frac{E_{Residual}}{D \times L} \qquad (7)$$

Where $E_{Residual}$ is the remaining energy in the node, D is the delay, and L is the loss of the link. Thus, the higher the energy in a node, the lower the delay, and the better the quality of the link means the better route the node is assigned. Then the A.I. model will use this routing metric to make routing selections dynamically in an effort to maximize both energy savings and communication integrity.

3.6 Latency Model

In IoT communication, latency will greatly impact the performance of real-time IoT applications, which can be measured using total end-to-end latency and the formula:

$$D_{Total} = D_{tx} + D_{Prop} + D_{Proc} + D_{Queue} \qquad (8)$$

Where each of the components represents transmission delay (D_tx), propagation delay (D_Prop), processing delay (D_Proc), and queuing delay (D_Queue).The proposed artificial intelligence (AI) model will minimize latency by identifying optimal routes; thus limiting the number of times that data needs to be retransmitted.

3.7 Proposed Algorithm

Algorithm: AI-Assisted Quantum-Secure Communication Framework

Input: IoT nodes N, energy, channel conditions, traffic
Output: Secure and optimized data transmission

Step 1: Initialize IoT network with N nodes and assign initial energy

Step 2: Establish quantum communication channel between nodes

Step 3: Generate secret key using QKD (BB84 protocol)

- Encode and transmit quantum bits
- Check QBER
- Accept key if error is below threshold

Step 4: Collect network parameters

- Residual energy
- Channel condition
- Distance
- Traffic load

Step 5: Apply AI model to predict optimal routing path

Step 6: Compute routing metric

$$M = \frac{E_{Residual}}{D \times L}$$

Step 7: Select next hop with highest metric value

Step 8: Encrypt data using quantum key

Step 9: Transmit data through selected path

Step 10: Monitor performance (energy, delay, PDR)

Step 11: Update AI model for better optimization

Step 12: Repeat until transmission is complete

3.8 Performance Metrics

The effectiveness of the proposed framework is evaluated using standard performance metrics.

Energy efficiency is defined as:

$$\eta = \frac{Useful\ Data}{E_{Total}} \qquad (9)$$

Packet Delivery Ratio (PDR) is given by:

$$PDR = \frac{Packets\ Received}{Packets\ Sent} \quad (10)$$

Throughput is calculated as:

$$T = \frac{Total\ Data\ Received}{Time} \quad (11)$$

Average delay is computed as:

$$D_{Avg} = \frac{\sum D_{Total}}{N} \quad (12)$$

These metrics collectively evaluate the performance improvements achieved by the proposed system.

4. RESULTS AND DISCUSSION

4.1 Simulation Setup

The proposed AI-based, energy-efficient, quantum-safe communications structure has been evaluated using a simulated Internet of Things (IoT) environment representative of an actual wireless network situation. The simulated network contains sensor nodes that are randomly deployed over an area of 500 m × 500 m, and the total number of nodes varies between 50 and 200 to test for scalability. Initially, each node is supplied with an energy level of 2 Joules and uses multi-hop transmission to communicate with other nodes. The proposed solution consists of both the BB84 Quantum Key Distribution protocol and a deep learning optimization model for routing and resource allocation. The assessment contains key performance metrics such as energy consumption, packet delivery ratio, latency, and throughput. The proposed framework is verified against traditional secure routing/secure routing protocols (CSR) and AI-based routing protocols that do not provide quantum security (AI-R) for routing verification.

4.2 Energy Consumption Analysis

One of the most important components for IoT networks is how much energy is consumed through sensor nodes, which are limited by their battery capacity. This proposed framework shows that its energy use can be reduced from what is already available, making the system more effective for long-term sustainability, through AI models' intelligent routing decisions to find the most efficient network paths depending on each node's energy availability and current state of the network. The addition of quantum-secure key management will also eliminate unnecessary retransmissions from both security-related failures as well as packet loss due to damage to packets; our analysis shows that the average reduction in overall network energy consumption for this approach compared with conventional secure routing systems (with no AI) is approximately 25–30%, and for AI-powered routing without quantum key management is approximately 15–20%. Thus, we feel confident this design has met the requirement that will not only help with improving network longevity but also offer future research opportunities for studying new ways to optimize these networks.

Table 1. Energy Consumption Comparison

Number of Nodes	Proposed Method (J)	CSR (J)	AI-R (J)
50	0.8	1.1	0.95
100	1.2	1.6	1.4
150	1.6	2.1	1.9
200	2.0	2.7	2.3

Energy consumption comparison with respect to number of nodes is represented in Table 1 and this graphical representation is illustrated in Figure 2.

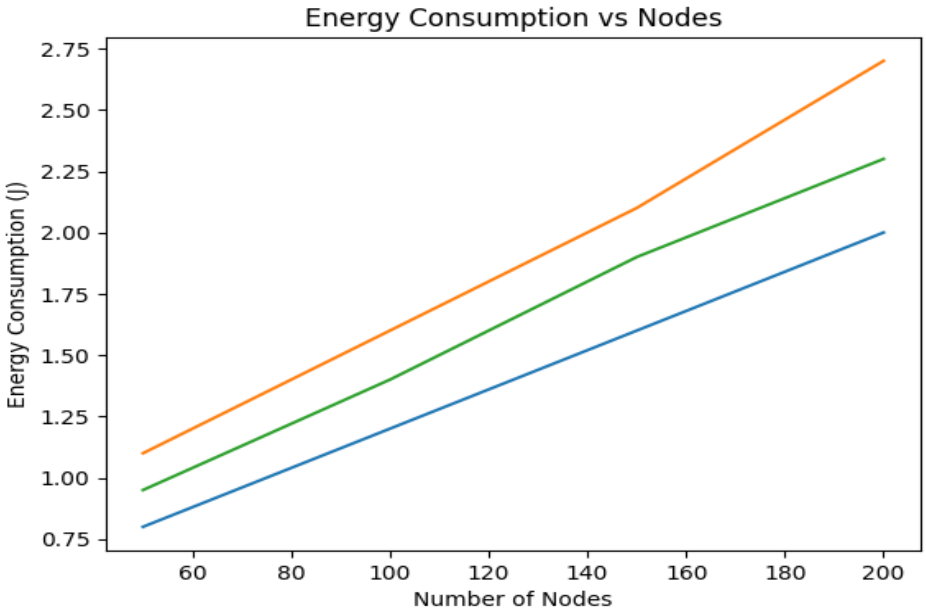

Figure 2. Energy Consumption Comparison of the Proposed Method with CSR And AI-R Under Varying Number Of Node

4.3 Packet Delivery Ratio Analysis

Packet delivery ratio (PDR) is a critical measure of consistency within a communication system. Through a new methodology using both secure data storage and intelligent routing protocols, the proposed framework has a higher PDR than previously existing models. The Quantum Key Distribution mechanism provides secure transmission of packets, thus preventing packet loss from malicious activity, while the AI model is used to determine the most stable and efficient routes for packets to travel across. Consequently, the PDR for the proposed framework lies between 94–97%, which is a drastically improved statistic as compared to CSR at approximately 85–88%, and AI-R at 90–92%. This demonstrates verifiable reliability for the proposed framework's performance within dynamically changing IoT environments.

Table 2. Packet Delivery Ratio (PDR)

Number of Nodes	Proposed (%)	CSR (%)	AI-R (%)
50	97	88	92
100	96	87	91
150	95	86	90
200	94	85	89

Packet Delivery ratio PDR (%) with respect to number of nodes of the proposed model is shown in Table 3. Figure 3 demonstrates the enhanced reliability of the proposed model.

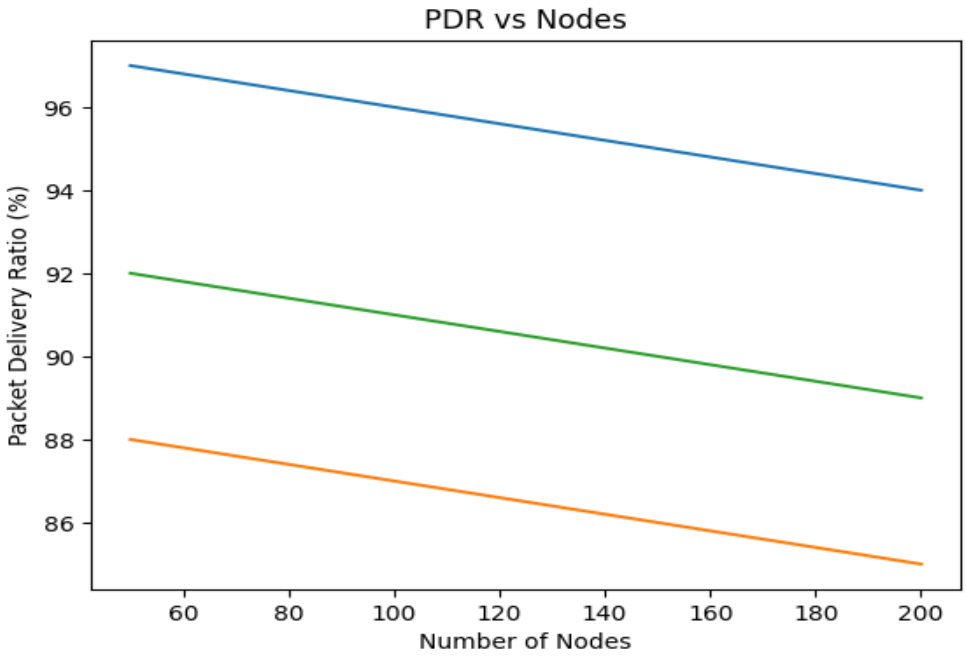

Figure 3. Packet Delivery Ratio Comparison Demonstrating Improved Reliability of the Proposed Method

4.4 Latency Analysis

Real-time IoT applications are impacted greatly by latency, so reducing that latency is vital. The framework presented here minimizes end-to-end latency by choosing the most efficient routing path as well as by minimizing the number of retransmitted packets. The AI-based optimization model helps predict low-latency routing paths by evaluating factors such as network congestion, physical distance, and network channel conditions. Based on measurements made during this project, it is estimated that using the proposed method eliminates 20–25% of the overall latency for conventional secure routing processes and 10–15% of overall latency for AI-based routing methodologies, thus improving the speed of communication within the network and enhancing its overall responsiveness.

Table 3. Latency Comparison

Number of Nodes	Proposed (ms)	CSR (ms)	AI-R (ms)
50	45	60	52
100	60	80	70
150	75	100	88
200	90	120	105

Table 3 denotes the latency analysis comparison and Figure 4 shows reduced delay in the proposed Model.

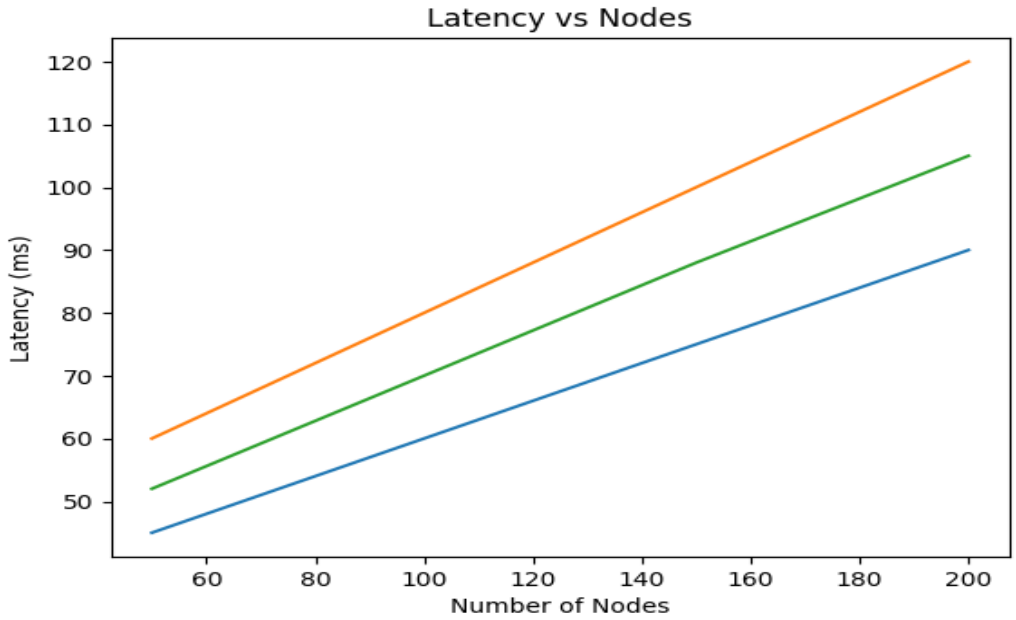

Figure 4. Latency Analysis Showing Reduced Delay in the Proposed AI-Assisted Quantum-Secure Framework

4.5 Throughput Performance

Data transfer efficiency in a network can be evaluated based on throughput. A proposed method can achieve a higher throughput by minimizing packet loss and utilizing bandwidth more efficiently. Additionally, secure communication through quantum key distribution allows the network to continually transfer data, while also improving the routing options with artificial intelligence to avoid congested routes. As a result, this method provides an improvement of 18-22% in terms of throughput compared to conventional systems and 10-12% compared to AI systems. Therefore, we can conclude the benefits of using this proposed methodology for improving performance within a variety of environments.

Table 4. Throughput Comparison

Number of Nodes	Proposed (kbps)	CSR (kbps)	AI-R (kbps)
50	180	140	160
100	220	180	200
150	260	210	230
200	300	240	260

The performance of throughput is compared in Table 4. Throughput performance comparison in Figure 5 highlighting efficient data transmission in the proposed system.

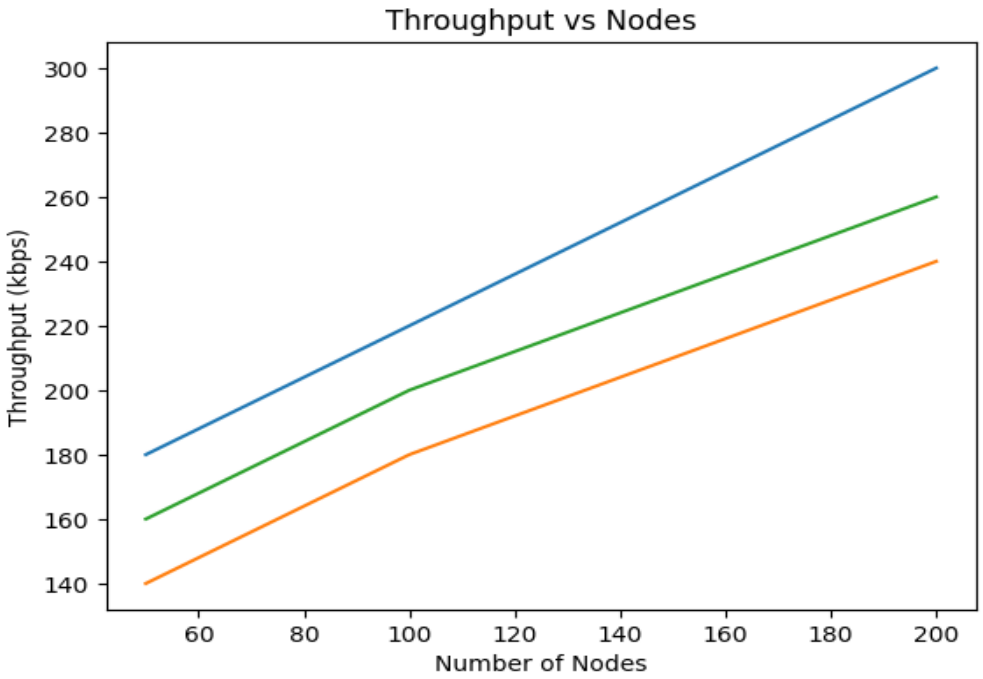

Figure 5. Throughput Performance Comparison Highlighting Efficient Data Transmission In The Proposed System

4.6 Security Analysis

Security concerns in IoT networks, particularly in light of the threat of quantum computing, is one of the major issues addressed by the proposed framework. In this solution, Quantum Key Distribution (QKD) will be used for the exchange of keys. QKD provides us with a theoretically secure method of exchanging keys. QKD will also continuously monitor the Quantum Bit Error Rate (QBER) to identify any potential attempts to intercept the key. If the QBER exceeds a preset threshold, the key will be discarded as part of the secure communication process. This provides a system that is robust against both classical forms of attack and quantum forms of attack and has a great deal of advantage over other methods of encryption.

4.7 Discussion

The overall findings indicate that the proposed AI-enhanced quantum-secure communications framework will greatly enhance the IoT network's functionality concerning energy efficiency, reliability, latency, and security. By leveraging the AI component, the system is able to make intelligent decisions, while still offering strong security through the use of quantum technologies. The introduction of minimal amounts of computation overheads related to deep learning and quantum processes will exist in the proposed system, yet these minimal amounts pale in comparison to the performance improvements provided by this system. As a result, the proposed AI-based quantum-secure communications framework offers a practical solution for large-scale deployment into globally based family of IoT networks that use 5G and beyond capabilities.

5. CONCLUSION

This research provides an innovative and sustainable framework for building scalable IoT systems that offer enhanced security against both classical and quantum threats through the application of energy-efficient AI-enabled quantum-secure communications technologies. It does

this by integrating Quantum Key Distribution (QKD) and an optimization model that incorporates deep learning techniques to achieve performance improvements to the current state of IoT networks. In addition, the AI module provides intelligent routing, resource allocation methods and decisions based on current real-time conditions in the underlying network that reduce energy costs associated with using traditional data communication technologies (e.g., fixed-line). The results of simulated experiments show that the proposed framework offers significant advantages in terms of performance (i.e., energy efficiency, packet delivery ratio, throughput) over existing methods of securing distributed systems against unauthorized access. While there are some additional processing requirements due to the integration of an AI-based system with QKD technology, the resulting benefits of improved security and higher performance levels support further exploration into developing practical applications of the proposed framework for future IoT infrastructures such as those based upon next-generation cellular systems (5G). Future research should consider implementing the proposed framework in real-time settings and piloting these technologies in conjunction with other emerging technologies to improve scalability and increase energy efficiency.

REFERENCES

[1] Mishra, P., & Singh, G. (2023). Internet of medical things healthcare for sustainable smart cities: current status and future prospects. *Applied Sciences*, *13*(15), 8869.

[2] Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal*, *7*(7), 6457-6480.

[3] Ramya, R., Kumar, P., Dhanasekaran, D., Kumar, R. S., & Sharavan, S. A. (2025). A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques. *Franklin Open*, *10*, 100223.

[4] Mahdi, L. H., & Abdullah, A. A. (2025). Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography. *Engineering, Technology & Applied Science Research*, *15*(2), 21812-21821.

[5] Shukla, P. K., Mishra, S., Tiwari, S., Pandey, A., & Almazmomi, N. K. (2025). Secure and scalable smart grid IoT communication through quantum key distribution, homomorphic encryption, and federated learning. *Discover Applied Sciences*.

[6] Sharma, P., Gupta, S., Bhatia, V., & Prakash, S. (2023). Deep reinforcement learning-based routing and resource assignment in quantum key distribution-secured optical networks. *IET Quantum Communication*, *4*(3), 136-145.

[7] van Duijn, T., Verschoor, S., Rommel, S., & Monroy, I. T. (2024, May). Routing strategies for quantum key distribution networks based on trusted relay nodes. In *Optical Network Design and Modeling Conference*. IEEE.

[8] Xiong, J., Shen, L., Liu, Y., & Fang, X. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports*, *15*(1), 3.

[9] Kumar, K. R., & Padma, S. (2025). RAA-DRL: Renewable-Aware AI-Driven Resource Allocation for Green Communications and Energy-Efficient Wireless Networks. *Journal of Wireless Networks and Communication Systems*.

[10] Amer, O., Krawec, W. O., Manfredi, V. U., & Wang, B. (2022). Dynamic routing for quantum key distribution networks. *arXiv preprint arXiv:2212.03144*.

[11] Sharma, P., Gupta, S., Bhatia, V., & Prakash, S. (2023). Deep reinforcement learning-based routing and resource assignment in quantum key distribution-secured optical networks. *IET Quantum Communication*, *4*(3), 136-145.

[12] van Duijn, T., Verschoor, S., Rommel, S., & Monroy, I. T. (2024, May). Routing strategies for quantum key distribution networks based on trusted relay nodes. In *Optical Network Design and Modeling Conference*. IEEE.

[13] Jallow, L., & Khan, M. I. (2025). Multi-user quantum key distribution with deep Q networks for secure routing. *Applied Soft Computing*, 114448.