IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15724

# Quantum Key Distribution for Secure IoT Communication: Recent Advances, Challenges, and Future Perspectives

**Sivasubramanyam Medasani[1], Akhil Goutham K[2], Bhaskar S[3], H Vishnu[4]**

Professor, Computer Science and Engineering, K. S. School of Engineering and Management, Bengaluru, India[1]

Student, Computer Science and Engineering, K. S. School of Engineering and Management, Bengaluru, India[2]

Student, Computer Science and Engineering, K. S. School of Engineering and Management, Bengaluru, India[3]

Student, Computer Science and Engineering, K. S. School of Engineering and Management, Bengaluru, India[4]

**Abstract**: The rapid proliferation of Internet of Things devices (IoT) across healthcare, smart homes, transportation, and industrial automation has led to an unprecedented exchange of sensitive data over wireless channels, exposing these networks to cyberattacks, eavesdropping, and unauthorized access. Conventional cryptographic techniques, which rely on computational hardness assumptions, are increasingly vulnerable to the emerging capabilities of quantum computing. This paper explores the application of Quantum Key Distribution (QKD) as a means of enabling secure and dependable data communication for IoT devices. By exploiting the fundamental principles of quantum mechanics, QKD allows two communicating parties to generate a shared secret key while inherently detecting any attempt at interception. The proposed approach aims to enhance data privacy, ensure secure authentication, preserve confidentiality, and safeguard IoT systems against present and future quantum enabled threats. The integration of quantum based security techniques into existing IoT infrastructure is examined, along with its implications for improving the reliability and trustworthiness of wireless IoT communication systems. This work positions Quantum Enhanced Secure Data Communication as a forward looking security solution for next generation IoT networks.

**Keywords:** Quantum Key Distribution, Internet of Things, Quantum Internet of Things, Post Quantum Cryptography, BB84 protocol, Quantum Cryptography Framework.

## I. INTRODUCTION

The IoT has transformed everyday environments by connecting a vast array of sensors, actuators, and embedded devices that continuously collect and exchange data. Applications ranging from remote patient monitoring and smart home automation to intelligent transportation and industrial control systems depend heavily on the timely and secure transmission of this data. However, the same connectivity that enables these applications also introduces significant security vulnerabilities. IoT devices often operate with limited computational resources, constrained power budgets, and simplified communication protocols, making them attractive targets for cyberattacks, data interception, and unauthorized access.

Traditional security mechanisms for IoT rely predominantly on classical cryptographic algorithms whose strength is based on the computational difficulty of certain mathematical problems. While such methods have served conventional networks reasonably well, the anticipated arrival of large scale quantum computers threatens to render many of these algorithms obsolete, since quantum algorithms can solve the underlying mathematical problems considerably faster than classical computers. This looming threat necessitates the exploration of quantum resilient security solutions capable of protecting sensitive IoT data both today and in a post quantum future.

QKD offers a promising alternative by leveraging the laws of quantum mechanics, rather than computational complexity, to guarantee the security of key exchange. Because any attempt to intercept or measure a quantum state inevitably disturbs it, QKD allows communicating parties to detect eavesdropping and establish a provably secure shared key. This paper investigates how QKD can be adapted and integrated into IoT communication architectures to deliver secure, reliable, and future proof data exchange across diverse smart applications.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15724

## II. RELATED WORKS

Evolving methodologies in quantum resistant access control were extensively mapped, who evaluated the structural viability of post quantum authentication and key agreement frameworks. This research meticulously details the dynamic landscape of modern quantum secure protocols, balancing a rigorous assessment of cryptographic features with their inherent computational burdens. Beyond categorizing existing vulnerabilities, their analysis highlights key gaps in the scalability of universal defenses, calling for accelerated development in lightweight post quantum primitives and secure quantum cloud infrastructures [1]. The paradigm of securing IoT ecosystems against evolving adversarial architectures has drawn substantial research interest. Several frameworks have been explored to bridge the gap between classical lightweight topologies and quantum safe communications. The QIoT using a BB84 based infrastructure to address key scarcity over resource constrained networks. This approach validated the utility of utilizing virtual key pools at edge gateways, yet noted deployment friction under severe device heterogeneity.

Addressing the computational bottlenecks of migrating multi node IoT environments to quantum safe architectures, a hybrid security framework combining Multi Node QKD with ECC. The protocol enforces end to end protection through structured pre deployment, registration, login, and authentication phases. Simulated performance benchmarks in Qiskit show that the architecture reduces encryption overhead and boosts key generation efficiency over standard ECC. Furthermore, the model establishes strong resilience against post quantum threats, maintaining a defense rate against simulated quantum attacks while preserving high scalability and low latency [2].

To solve transmission limitations over specialized physical mediums, deployed QKD via Free Space Optics (FSO) to establish high data rate secure communication loops between servers and IoT controllers in fast moving high speed train (HST) environments. Which demonstrates the physical properties of photon exchange links could effectively shield vulnerable peripheral nodes without deteriorating the consumer quality of service [3]. Empirically evaluating the concrete performance and network impact when transitioning IIoT systems to PQC [5].

A multi layered structure combining QKD, Homomorphic Encryption, and Federated Learning to resolve quantum vulnerabilities and computational bottlenecks in smart grids [6].The transition toward standardizing quantum architectures across varying domains has also exposed specific practical tradeoffs, a comprehensive survey on key management approaches within trusted repeater QKD networks, establishing that while such systems yield Information Theoretically Secure (ITS) key agreements, real time synchronization remains tightly constrained by classic physical distance limitations. Similarly, quantum key mechanism as enforce data privacy and self healing authentications within Smart Grids, identifying that high processing delays can inadvertently slow anomaly detection windows if session key renewals are unoptimized [8].

Secure communication underpins the widespread adoption of modern telecommunication networks and services. As advances in computing power and mathematical techniques continue to accelerate, the search for robust cryptographic solutions has become increasingly critical.QKD has emerged as a promising technology capable of offering Information Theoretically Secure (ITS) key agreement between two remote parties, a guarantee rooted in the fundamental laws of quantum mechanics rather than computational assumptions. To extend this capability beyond simple point-to-point links, QKD networks employing trusted relay nodes have been developed, enabling secure key distribution to a larger number of participants across arbitrary distances. These networks operate as a complementary layer atop conventional communication infrastructure, responsible for generating, managing, and supplying ITS cryptographic keys to end users. However, because quantum key generation resources are inherently limited, the integration of QKD network services into critical infrastructure demands careful and efficient key management strategies to ensure reliable, scalable operation [9].

Furthermore, a hybrid quantum classical security model that offloads processing overhead by splitting lightweight QKD protocols onto peripheral sensors while scheduling heavy deep packet inspection via quantum neural networks on centralized edge servers.

On the other note some developed an energy efficient QCF tailored for wireless IoT environments, verifying that integration with classical communication protocols successfully guarantees forward secrecy and resistance to future quantum cryptanalysis.

Lastly, some highlighted that while PQC provides mathematical alternatives, direct implementation of physical hardware like Quantum Random Number Generators (QRNGs) and QKD links remains the definitive method to completely prevent "harvest now, decrypt later" attacks across critical fields such as smart healthcare and industrial automation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15724

## III. COMPARATIVE ANALYSIS

Classical cryptography remains the most practical choice for resource constrained IoT endpoints today but offers no protection against future quantum capable adversaries, making it vulnerable to "harvest now, decrypt later" attacks. PQC provides a quantum resistant alternative that is more compatible with existing IoT hardware and network infrastructure, since it relies on mathematical hardness assumptions rather than specialized physical equipment, though it still depends on unproven long term security against undiscovered quantum algorithms. QKD offers the strongest theoretical security guarantee, rooted in physics rather than computational hardness, but its range limitations, cost, and infrastructure demands currently restrict it to high value, security critical backbone links rather than pervasive IoT deployment. The reviewed studies demonstrate the growing adoption of quantum enhanced cryptographic techniques for securing IoT networks. To facilitate a clear comparison, Table I summarizes the methodologies, key contributions, and limitations of the existing research.

| Method / Technique | Key Contribution | Limitations |
|---|---|---|
| Post Quantum Authentication and Key Agreement Frameworks [1] | Analyzed quantum resistant access control mechanisms and identified scalability challenges in post quantum cryptography. | High computational complexity and lack of lightweight PQC solutions. |
| Multi Node QKD with ECC [2] | Improved key generation efficiency, reduced encryption overhead, and enhanced scalability for IoT security. | Requires dedicated QKD infrastructure and complex deployment. |
| BB84 based QKD over Free Space Optics (FSO) [3] | Enabled secure high-speed communication between IoT controllers and servers in HST environments. | Performance depends on line of sight and environmental conditions. |
| BB84 based QIoT Framework [4] | Introduced virtual key pools for secure communication in resource constrained IoT networks. | Device heterogeneity affects implementation efficiency. |
| Post Quantum Cryptography (PQC) for IIoT [5] | Evaluated the performance impact of PQC adoption in Industrial IoT systems. | Increased computational and communication overhead. |
| QKD + Homomorphic Encryption + Federated Learning [6] | Enhanced privacy, secure computation, and collaborative learning for smart grids. | High computational complexity and resource requirements. |
| Trusted Repeater QKD Networks [7] | Achieved information theoretically secure key management in quantum networks. | Limited transmission distance and synchronization issues. |
| QKD based Smart Grid Authentication [8] | Improved authentication and data privacy through secure session key management. | Frequent key renewal increases processing latency. |
| Hybrid Quantum Classical Security Framework [9] | Reduced IoT device overhead by combining lightweight QKD with edge based quantum neural networks. | Requires powerful edge computing resources. |
| Energy Efficient Quantum Communication Framework (QCF) [10] | Provided forward secrecy and resistance against future quantum attacks in wireless IoT. | Integration with legacy communication protocols remains challenging. |
| QRNG and QKD Based Security [11] | Eliminated "Harvest Now, Decrypt Later" threats using quantum hardware based security. | High implementation cost and specialized hardware requirements. |

## III. RESEACRH GAPS

**A. Absence of Lightweight QKD Compatible Protocols for Constrained Devices:** Existing QKD implementations assume relatively capable endpoints capable of handling reconciliation, error correction, and privacy amplification.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15724

Little research addresses how extremely resource constrained IoT devices can participate in or benefit from QKD secured sessions without excessive computational or energy overhead, beyond simple key offloading [1, 2, 5, 8].

**B. Lack of Standardized Hybrid Quantum Classical Architectures:** While hybrid models combining QKD with classical/PQC cryptography are widely proposed conceptually, there is no unified, standardized architecture specifying how key handoff, session management, and protocol negotiation should occur between the quantum backbone and classical IoT edge layers. Most existing work treats these as loosely coupled systems rather than an integrated stack [3, 4 ,5, 7].

**C. Limited Real World Performance Data Under Realistic Network Conditions:** Much of the existing literature relies on simulation based QBER and key rate analysis under idealized or laboratory conditions. There is a gap in empirical studies evaluating QKD IoT hybrid systems under real world network impairments latency jitter, packet loss, concurrent multi device load, and fluctuating channel noise particularly over actual TCP/IP infrastructure as opposed to purely theoretical channel models [2, 3, 4, 7].

**D. Insufficient Research on Scalable Key Management for Massive IoT Deployments:** Current QKD key management frameworks are largely designed for point to point or small trusted node networks. Research addressing how QKD derived key material can be efficiently distributed, cached, and refreshed across thousands or millions of concurrent IoT sessions without exhausting limited quantum key generation throughput remains under developed [4, 10].

**E. Underexplored Security of Trusted Relay Nodes in IoT Specific Contexts:** While trusted node vulnerabilities are acknowledged generally in QKD literature, few studies specifically model the threat surface of trusted relays within heterogeneous, multi vendor IoT ecosystems, where relay nodes may span different administrative domains, trust levels, and physical security postures [4,10].

**F. Lack of Integrated Test beds Combining BB84 Simulation with Live Network Transport**: Most academic QKD IoT studies either simulate the quantum layer in isolation or model the classical network layer separately, with few implementations demonstrating a fully integrated pipeline from quantum key generation through TCP based classical key confirmation to actual AES encrypted IoT sensor data transmission as attempted in this project [2, 3, 7, 8].

**G. Minimal Study of Eavesdropping Detection Response in Operational IoT Settings:** While intercept-resend attack detection via QBER thresholds is well established theoretically, research is limited on how IoT systems should practically respond to detected eavesdropping in real time e.g., automatic session abort, fallback protocols, device quarantine, or alerting mechanisms without disrupting time sensitive IoT operations [2, 4, 6].

**H. Absence of Cost Benefit and Energy Efficiency Models for QKD IoT Adoption:** There is limited quantitative research modeling the trade off between the security gains of QKD integration versus its energy, latency, and infrastructure cost overhead specifically for IoT use cases, making it difficult for practitioners to justify adoption decisions with data driven evidence [1, 2, 3, 8].

**I. Limited Cross Layer Optimization Between QKD Key Refresh Rates and Application Layer QoS:** Few studies address how varying QKD key generation/refresh rates should be dynamically matched to the quality of service (QoS) requirements of different IoT application classes, rather than applying a uniform refresh policy [3, 4, 7].

**J. Sparse Evaluation of PQC as a Fallback During QKD Unavailability:** While PQC is often mentioned as a complementary technology, limited research explores seamless failover mechanisms where an IoT system dynamically switches between QKD derived keys and PQC derived keys during quantum channel outages or trusted node failures, without compromising session continuity or security guarantees [1, 4, 6]

## IV. CHALLENGES AND LIMITATIONS

**A. Distance Limitations:** QKD relies on transmitting individual photons, which are highly susceptible to attenuation and scattering in optical fiber. This restricts QKD links to a limited operational range without intermediate repeaters, beyond which signal loss makes secure key generation unreliable. This poses a major constraint for wide area IoT deployments spread across large regions like power grids or smart cities. Overcoming this requires quantum repeaters or strategically placed trusted relay nodes, both adding cost and complexity [2, 3, 10].

  

DOI: 10.17148/IJARCCE.2026.15724

**B. Lack of Quantum Repeaters:** Practical, scalable quantum repeaters capable of extending range without violating the no cloning theorem remain largely experimental. In their absence, network architects rely on "trusted nodes" that decrypt and re encrypt keys at intermediate points, enabling longer distance distribution. However, this reintroduces classical security assumptions and creates potential compromise points. For IoT applications needing long term confidentiality, such as healthcare or critical infrastructure, this significantly undermines QKD's core security guarantee [2, 3, 10].

**C. Low Key Generation Rate:** QKD protocols like BB84 generate keys at much lower rates than classical methods due to the probabilistic nature of quantum measurement and reconciliation overhead. This is often insufficient for IoT ecosystems generating continuous, high volume sensor data, such as video surveillance or industrial telemetry. This mismatch necessitates hybrid strategies, including pre generating and buffering keys, or reserving QKD derived keys only for the most security critical control messages [3, 4, 7].

**D. High Infrastructure Cost:** Deploying QKD requires specialized, expensive hardware single photon sources, sensitive detectors, precision timing electronics, and dedicated optical channels. Unlike classical cryptography, which runs on standard computing hardware, QKD demands costly purpose built infrastructure. This makes it economically unviable to equip every IoT sensor with QKD capability at mass scale. As a result, adoption is currently justifiable only for high value, security critical network segments rather than pervasive deployment [2, 3, 8].

**E. Device Resource Constraints:** Most IoT devices have strict limitations on processing power, memory, and battery life to remain small and energy efficient. Running QKD directly on such devices is infeasible, since it requires precise optical alignment and computationally intensive post processing like error correction. QKD must therefore be confined to capable infrastructure like gateways or edge servers, which distribute classically encrypted symmetric keys to resource constrained end devices, limiting the security guarantee to the last mile classical link [1, 2, 5].

**F. Integration Complexity:** IoT ecosystems run on a heterogeneous mix of protocols TCP/IP, MQTT, CoAP, and 5G/6G cores none originally designed with QKD in mind. Integrating QKD requires substantial architectural redesign, including middleware for key exchange and synchronization between quantum and classical channels. This demands cross disciplinary expertise spanning quantum physics, networking, and software development. Poor design can introduce timing mismatches or vulnerabilities that negate QKD's security benefits [3, 4, 5, 7].

**G. Vulnerability of Trusted Nodes:** In multi hop QKD networks, trusted relay nodes must decrypt and re-encrypt keys before forwarding them, giving each node full access to plaintext key material. This creates a potential single point of failure if any node is compromised, hacked, or malicious, the entire network's security guarantee is undermined. This is especially concerning for IoT applications spanning multiple administrative domains. Mitigation requires multi path key routing, node redundancy, and rigorous physical security auditing [4, 10].

**H. Environmental Sensitivity:** Free space QKD, which transmits photons through open air rather than fiber, is highly sensitive to weather, atmospheric turbulence, fog, and ambient light interference. These factors cause photon loss and signal degradation, reducing channel reliability. This poses a particular challenge for mobile and outdoor IoT use cases like V2X communication, drone swarms, or satellite links requiring stable line of sight. This limits QKD's reliability for continuous, always on security in dynamic outdoor environments [2, 8, 12].

**I. Lack of Standardization:** The QKD industry lacks universally accepted protocols and interoperability standards, with vendors often implementing incompatible proprietary systems. This fragmentation complicates building multi-vendor, cross-platform IoT security architectures at scale. While bodies like ETSI have begun developing QKD standards, these efforts remain evolving and not yet widely adopted. This creates uncertainty for organizations investing long-term, risking vendor lock in or premature obsolescence [2, 6, 14].

**J. Side Channel Attacks and Scalability:** Despite offering information theoretic security at the protocol level, real world QKD implementations remain vulnerable to hardware level side channel attacks like detector blinding, which exploit physical device imperfections. Additionally, current QKD architectures, designed mainly for point to point or small trusted node networks, are not yet equipped for the massive scale of billions of devices envisioned in 6G IoT ecosystems. Addressing both gaps requires continued research into device independent protocols and more efficient, scalable network architectures [4, 5, 16].

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15724

## V. FUTURE REASEARCH DIRECTIONS

**A. Development of Lightweight QKD Aware Protocols for Constrained Devices:** Future work can explore ultra lightweight key confirmation and session establishment protocols specifically designed for microcontroller based IoT endpoints, minimizing computational and energy overhead while still leveraging QKD derived keys distributed from gateway nodes [1, 2, 5].

**B. Standardized Hybrid Quantum Classical Architecture Design:** Research can focus on formalizing a unified reference architecture potentially proposed for IEEE or ETSI standardization that clearly defines interfaces, handoff procedures, and session management protocols between the QKD backbone and classical IoT edge layers [3, 4, 5, 7].

**C. Real World Deployment and Field Testing:** Extending the current simulation based implementation to a physical testbed using actual quantum hardware or quantum cloud services, combined with real IoT hardware and live network conditions, would validate performance beyond simulated environments [2, 3, 4, 7].

**D. Scalable Multi Device Key Management Frameworks:** Future research can investigate distributed key caching, hierarchical key management, and load balancing strategies to support hundreds or thousands of concurrent IoT devices sharing a limited QKD key generation resource, potentially using SDN based orchestration [4, 10].

**E. Integration of Post Quantum Cryptography as a Resilient Fallback:** A valuable extension involves designing and testing automatic failover mechanisms between QKD and PQC algorithms during quantum channel disruption, ensuring continuous secure operation without service interruption [1, 3, 5, 10].

**F. Machine Learning Based Anomaly and Eavesdropping Detection:** Beyond static QBER thresholds, future work can explore ML/AI driven anomaly detection models that analyze quantum channel behavior patterns over time to detect subtler or adaptive eavesdropping strategies, improving detection sensitivity and reducing false positives [2, 6, 7].

**G. Energy Aware and Cost Aware QKD Orchestration:** Research can develop quantitative models and simulation frameworks to optimize the placement and activation of QKD links based on energy consumption, infrastructure cost, and data sensitivity, enabling data driven decisions on where QKD deployment is most justified [1, 2, 7].

**H. Extension to Multi Hop and Mesh QKD IoT Networks:** Future studies can generalize the current point to point architecture to multi hop trusted relay or mesh topologies, evaluating key relay security, latency accumulation, and fault tolerance across larger, more realistic IoT network layouts [3, 4, 10]

**I. Integration with 5G/6G Network Slicing:** Investigating how QKD secured key distribution can be dynamically provisioned within 5G/6G network slices allocating dedicated quantum secured slices for high priority IoT traffic represents a promising direction aligned with next generation network architectures [5, 7].

**J. Formal Security Proofs and Side Channel Hardening**: Future work can pursue formal, composable security proofs for the complete hybrid protocol stack under realistic adversarial models, along with hardware level countermeasures against side channel attacks such as detector blinding [2, 4, 5].

**K. Satellite and Free Space QKD for Remote IoT Deployments**: Extending the architecture to incorporate satellite based or free space optical QKD could enable secure key distribution to remote or mobile IoT deployments that lack fiber optic infrastructure [2, 3, 10].

**L. Usability and Deployment Cost Studies for Industry Adoption:** Future research can conduct case studies or pilot deployments with industry partners to assess real world usability, integration effort, and total cost of ownership, helping bridge the gap between academic prototypes and commercial adoption [1, 2, 7, 10].

## VI. CONCLUSION

A critical and growing challenge in the field of IoT security the vulnerability of traditional encryption methods to the increasing threat posed by quantum computers. Existing hybrid security models, while promising, tend to suffer from

  

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026
DOI: 10.17148/IJARCCE.2026.15724

high latency, excessive energy consumption, and implementation difficulties on resource constrained edge IoT devices, which formed the core of our problem statement.

To address this, we conducted an in depth literature survey covering five recent research papers which helped us understand the current landscape of QKD, PQC, and their applicability to IoT environments. Through this study, we gained clarity on the research gaps particularly the need for lightweight, efficient, and quantum safe communication frameworks.

Based on these insights, we have defined a clear set of objectives for our project. We aim to implement the BB84 QKD protocol in Python to simulate secure key generation, establish secure IoT communication using the MQTT protocol, and incorporate Machine Learning based anomaly detection to identify suspicious network behaviour. The ultimate goal is to bring together Quantum Computing, IoT communication, and Machine Learning into one unified and efficient secure communication system.

## REFERENCES

[1] P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT enabled applications: A comprehensive survey and open challenges," Computer Science Review, vol. 54, p. 100676, 2024.
[2] R. Chaturvedi, D. Sahu, B. P. Singh, S. Prakash, T. Yang, R. S. Rathore, K. Cengiz, and N. Ivković, "A hybrid multi-node QKD-ECC architecture for securing IoT networks," Scientific Reports, vol. 15, p. 32831, 2025.
[3] A. S. Parihar, "A secure communication in distributed system using quantum key distribution," The Journal of Supercomputing, vol. 81, no. 1468, 2025.
[4] Y. Yang, Y. Lin, J. Xiao, and Z. Zhong, "Feasibility discussion of quantum cryptography for Internet of Things security: a literature review," Optical and Quantum Electronics, vol. 57, no. 264, 2025.
[5] L. Cruz-Piris, A. Marín-López, M. Álvarez-Campana, M. Sanz, J. I. Moreno, and D. Arroyo, "Measuring the impact of post quantum cryptography in Industrial IoT scenarios," Internet of Things, vol. 34, p. 101793, 2025.
[6] Shukla, Prashant Kumar, Suchi Mishra, Sachin Tiwari, Ankur Pandey, and Najah Kalifah Almazmomi. "Secure and scalable smart grid IoT communication through quantum key distribution, homomorphic encryption, and federated learning." Discover Applied Sciences 8, Art. no. 162, 2026.
[7] Ganesh Babu R., Geetha T. S., Nedumaran A., Bashyam Sugumaran, and Muralikrishnan P. "Integrating quantum computing with federated learning for enhanced security and privacy in IoT networks." Results in Engineering 29 108500, 2026.
[8] Chawla, Diksha, and Pawan Singh Mehra. "A Survey on Quantum Computing for Internet of Things Security." Procedia Computer Science 218 2191–2200, 2023
[9] Dervisevic, Emir, Amina Tankovic, Ehsan Fazel, Ramana Kompella, Peppino Fazio, Miroslav Voznak, and Miralem Mehic. "Quantum Key Distribution Networks - Key Management: A Survey." ACM Computing Surveys 57, no. 10, Article 257, 2025.
[10] Abreu, Diego, David Moura, Christian Esteve Rothenberg, and Antônio Abelém. "QuantumNetSec: Quantum Machine Learning for Network Security." International Journal of Network Management 35 (2025): e70018.
[11] Kim, Tae Hoon, and S. Madhavi. "Quantum intrusion detection system using outlier analysis." Scientific Reports 14 27114, 2024.
[12] Amara, Marwen, Marwa Amara, Sami Mnasri, and Thierry Val. "QCNN-ID: A Quantum Classical Hybrid Model for IoT Intrusion Detection." Procedia Computer Science 2196 2204,2024
[13] Srinivasan, Kowshick, Aakanksha Trivedi, and Shuhui Yang. "Quantum-Enhanced Clustering for Intrusion Detection System in IoT Devices." In 2025 IEEE 22nd International Conference on Mobile Ad-Hoc and Smart Systems (MASS), pp. 610–615, 2025.
[14] Tawfik, Mohammed. "Optimized intrusion detection in IoT and fog computing using ensemble learning and advanced feature selection." PLOS ONE 19, no. 8 e0304082, 2024
[15] Bharathi, Indira, Veeramani Sonai, and Sridevi S. "Quantum-driven enhanced machine learning algorithm for intrusion detection in Internet of Things environment." EPJ Quantum Technology 13, no. 20, 2026.
[16] Kalinin, Maxim, and Vasiliy Krundyshev. "Security intrusion detection using quantum machine learning techniques." Journal of Computer Virology and Hacking Techniques 19 125–136, 2023.

  