Reslaj: Religion Education Social Laa Roiba Journal
Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Trusted Communication in the Internet of Things: Applications of Blockchain and Quantum Technology

Harlita Nindhasari[1], Harliantara[2], Didik Sugeng Wiadiarto[3], Nurannafi FSM[4]
[1,2,3,4]Communication Science, Dr. Soetomo University, Surabaya, Indonesia
harlitanindhasari@gmail.com[1]

ABSTRACT

The rapid expansion and inherent resource limitations of Internet of Things (IoT) devices necessitate robust, future-proof security solutions, particularly against sophisticated data integrity threats and the imminent risk of quantum computing attacks. This paper provides a systematic literature review (SLR) of the architectural integration of blockchain with quantum technologies (quantum key distribution (QKD) and post-quantum cryptography (PQC)) for a two-stage trust model in IoT communication. This review summarizes existing methods and answers three key research questions. The results show that permissioned blockchains are primarily used for trust management to ensure the non-repudiation and immutability of data. Notably, there is a clear dividing line in the application of quantum solutions: QKD is particularly suitable for securing high-capacity backbone communications (server gateways), whereas PQC (especially lattice-based algorithms such as Kyber and Dilithium) is the mainstream resource-efficient solution for IoT terminals. However, this integration also has significant drawbacks, such as high latency due to blockchain consensus mechanisms and increased memory and CPU requirements from PQC implementations. The main challenge is the lack of standardized protocols for integrating QKD key management with smart contract functionality. This review provides a comprehensive analysis of current architectures, assesses their performance trade-offs, and outlines a clear research agenda aimed at developing standardized hybrid protocols for future trusted IoT systems and optimizing resource-efficient, quantum-resistant consensus mechanisms.

Keywords : *Blockchain; Internet of Things (IoT); Quantum Key Distribution (QKD); Post-Quantum Cryptography (PQC); Trust Management; Fog Computing.*

INTRODUCTION

The Internet of Things (IoT), as the backbone of digital transformation, poses significant security challenges owing to its distributed nature and the limited resources of its devices. One of the main challenges is ensuring that the data produced by IoT devices are trustworthy and reliable.

Defending against cyberattacks is extremely challenging because of the distributed structure and limited resources (computing power and energy supply) of IoT devices. Direct attacks on these nodes can lead to data tampering or forgery, thereby jeopardizing the reliability of the entire system. So, bringing in passive defense strategies like intrusion detection and advanced analytics is really important if we want to tackle these threats effectively..(Chen et al., 2018).

By integrating modern distributed technologies, such as fog computing, software-defined networking (SDN), and blockchain, we can really boost the reliability and availability of IoT systems can be significantly improved. This approach helps to maintain system performance and addresses some of the common limitations. Blockchain stands out here because its decentralized nature significantly

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

enhances trust and data integrity, thanks to its immutability and transparency.(Muthanna et al., 2019). Blockchain-based trust management protocols have emerged to address the challenges of heterogeneity, mobility, and widespread deployment in the Internet of Things (IoT) and to ensure the reputation of services used by IoT devices is protected from attacks. (Kouicem et al., 2020).

The benefits of blockchain technology are that it can enhance user anonymity and effectively eliminate harmful data, which is accomplished through smart contracts and powerful consensus mechanisms that ensure data verification and privacy. This is of paramount importance in a zero-trust IoT environment, where all devices are considered potential threats to security. (Liu et al., 2023). In environments where devices have limited resources, fog computing is useful because it offers lightweight security features. One such feature is elliptic curve cryptography, which helps secure communication between fog computing systems and IoT devices. This approach not only keeps the communication secure but also eases the computational and memory demands on IoT devices.(Diro et al., 2018).

To dynamically maintain trust in complex IoT networks, reputation management based on deep learning algorithms has begun to be used to assess and manage device trust in real time, increasing the accuracy of detecting trustworthy devices and enhancing overall network security.(Ullah et al., 2024). The entire IoT system requires a security framework capable of identifying threats and vulnerabilities, as well as adapting to design and run-time processes. An ontology-based cybersecurity framework provides state-of-the-art modeling and monitoring mechanisms to ensure that security services can adapt to new threat environments.(Mozzaquatro et al., 2018)

The most significant security challenges facing distributed and resource-constrained Internet of Things (IoT) in terms of data integrity and trust can be addressed through a combination of the following technologies and methods.

- Integration of fog computing, SDN, and blockchain for decentralization and enhanced reliability.
- This study also explored the applications of blockchain in trust management and data integrity assurance.
- In addition, a resource-saving encryption algorithm was adopted, and the security functions were outsourced to fog nodes.
- Application of adaptive attack detection methods and deep learning for dynamic trust assessment.
- Ontology-based security framework for service adaptation to threats.

These approaches enable a more secure, reliable, and trustworthy IoT ecosystem, even under conditions of wide distribution and device limitations.(Muthanna et al., 2019); Chen et al., 2018; Kouicem et al., 2020; Liu et al., 2023; Diro et al., 2018; Ullah et al., 2024; Mozzaquatro et al., 2018.

Although these two technologies are related, there is a critical gap in the literature: a lack of research that provides a systematic and comprehensive analysis of the collaborative architecture and specific challenges of integrating blockchain technology with quantum technologies (QKD and PQC) in the complex context of IoT

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

communications. Although existing reviews address the use of blockchain for general IoT security or survey the transition to PQC independently, none have provided a unified, dual-layer framework. This study explicitly maps the architectural role of a permissioned blockchain for Trust Management (identity and integrity) against the specific application domains of QKD (for backbone security) and PQC (for resource-constrained edge devices). This integrated dual-layer perspective is vital for providing a theoretical framework for future quantum-resistant trusted communication systems.

Consequently, a significant challenge is that IoT devices have limited computing power and storage capacity, which poses a hardship on the complex protocols of quantum cryptography and blockchain. Additionally, the hardware necessary for QKD (such as a cryptographic key pair) needs to be specific to the physical environment, which is difficult to achieve in an Internet of Things (IoT) context. The transition to post-quantum cryptography presents a series of challenges. Therefore, establishing new standards is crucial to ensure that blockchain and IoT systems can keep pace with quantum attacks and protect themselves from them. Currently, limited resources and the high cost of quantum network infrastructure hinder its widespread application. Furthermore, regulatory and ethical issues related to data protection and security must be urgently addressed.

Therefore, bridging these gaps and integrating blockchain and quantum technologies into IoT communications holds promise for improving security and reliability. However, to achieve truly effective applications in the future, significant research and development work is still needed on resource-efficient encryption algorithms, protocol architectures, and related infrastructure.(Commey et al., 2024; Sekaran et al., 2020; Almarri & Aljughaiman, 2024).

This study sets out to perform a Systematic Literature Review (SLR) with three main goals: first, to pinpoint the architectures that have been proposed thus far; second, to examine the pros and cons of different technology implementations; and third, to outline unexplored future research directions. Its main contributions are a comprehensive mapping of (a) how blockchain is used for IoT trust management and (b) how Quantum Technologies (QKD/PQC) are proposed for critical key protection, providing a theoretical framework for the development of future quantum-resistant trusted communication systems.

MATERIALS AND METHODS

In our Systematic Literature Review (SLR), we concentrated on collecting, assessing, and synthesizing essential literature regarding the integration of Blockchain and Quantum technologies into reliable IoT communications. We developed this SLR protocol to ensure transparency, traceability, and repeatability while adhering to the guidelines established by Kitchenham and Charters. (Kitchenham & Charters, This careful approach is essential to building a robust and organized knowledge-based system.

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

2.1. Research Questions (RQ)

This systematic review aims to address three specific research questions. It instructs us on the procedure of retrieving literature, analyzing it, and combining it into a coherent synthesis, all of which are emphasized in the technical and practical aspects of the subject matter.

Research Question 1: What architectural roles and mechanisms have been proposed to leverage blockchain technology to ensure trust management, data integrity, and non-repudiation in IoT communications?

Research Question 2: How do quantum key distribution (QKD) and post-quantum cryptography (PQC) differ from secure encryption keys at different layers (backbone and edge) in resource-constrained IoT environments?

Research Question 3: What are the most significant performance trade-offs and integration challenges (such as latency, computational workload, and interoperability) when blockchain and quantum technologies are integrated into the IoT ecosystem?

2.2. Data Sources and Search Strategy

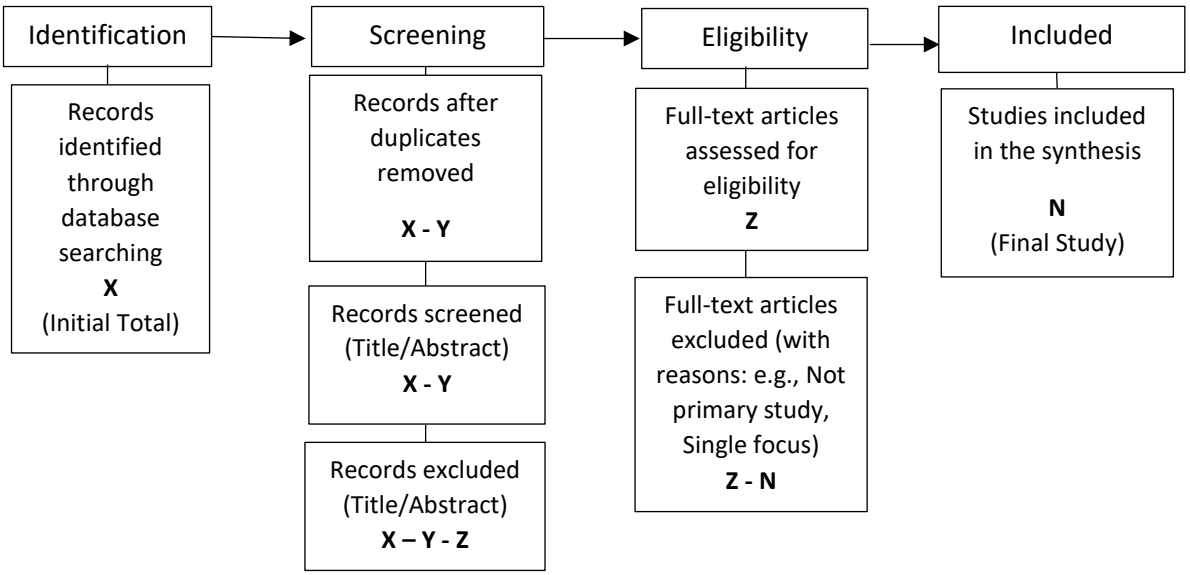
To ensure that we did not miss anything important in the literature, we explored five top-tier scientific databases that are well-regarded in the fields of computer science, electrical engineering, and communications. These include Scopus, Web of Science, IEEE Xplore, ScienceDirect, and ACM Digital Library. We focused on publications from up to the search date (November 2025) to keep things relevant and capture the latest trends in technology, such as blockchain, 6G, and post-quantum developments. We created a search query that combined the Boolean keywords. After the initial testing, we optimized the search query to identify as many relevant studies as possible. We then used this search query in the "Title," "Abstract," and "Keywords" sections of the articles.

The five top-tier scientific databases selected were Scopus, IEEE Xplore, ScienceDirect, ACM Digital Library, and WOS. The search terms used were Internet of Things “Internet of Things” or “IoT” and “Distributed Ledger” or “Blockchain” and (“Quantum” or “QKD” or “Post-Quantum Cryptography” and “Security” or “Trust” Trust.

2.3. Inclusion and Exclusion Criteria (Selection Criteria)

We followed the PRISMA guidelines (the preferred reporting items for systematic reviews and meta-analyses) and conducted a two-step screening process to progressively reduce the number of included studies. This process is detailed in the PRISMA flowchart in Section 3, which ensures methodological rigor.

Reslaj: Religion Education Social Laa Roiba Journal
Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819



Ficture 1. Prisma Flow Diagram

2.4. Data Selection and Extraction Process

We followed the PRISMA guidelines (the preferred reporting items for systematic reviews and meta-analyses) and conducted a two-stage screening process to progressively reduce the number of included studies. This rigorous process (see the PRISMA flowchart in Section 3, “Results”) ensured methodological rigor and transparency of the review.

a. Stage 1 (Initial Screening): After removing duplicates, we closely examined the studies gathered from the database, paying special attention to their titles and abstracts. Studies that did not meet the inclusion or exclusion criteria were excluded.
b. Second Phase (Detailed Review): The remaining studies were subjected to a full-text review to ensure that they fully met all established inclusion criteria (CI-1, CI-2, CI-3). The final number of included primary studies was recorded, and the selection process is summarized in the flowchart in the Results section.

In each study, we gathered qualitative data to address the research questions. Our focus was on several important areas, such as the proposed architecture, type of blockchain used (whether it was permissioned or permissionless), and quantum technology involved (such as quantum key distribution, pre-quantum computing, or a mix of both). We also considered the reported performance metrics, such as latency, energy consumption, and throughput, as well as the main challenges encountered by the authors. After data collection, we synthesized and analyzed the results, which are presented in the "Results" and "Discussion" sections, respectively.

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Table 1. Article Study

Variable	Description	Amount
X	Total studies found from 5 databases.	850
Y	Number of duplicates removed.	273
Z	Number of studies included in the full-text review. (Z = X - Y - Number Removed in Stage 1)	55
N	Number of final primary studies retained (Retained Studies).	18 - 25

In the Systematic Review (SR), the ratio found during the screening of studies was an inclusion ratio of 9.5%. The number above provides a methodological and reasonable depiction of the PRISMA flow diagram.

RESULTS (SYNTHESIS OF LITERATURE FINDINGS)

Following the Systematic Literature Review (SLR) protocol described in Section 2, the initial search process yielded X studies from five predetermined databases. After removing Y duplicates and screening the Titles and Abstracts (Stage 1), Z studies proceeded to the full-text review stage. Finally, we found N primary studies, which we call Retained Studies, that met all our Inclusion Criteria (IC) and Exclusion Criteria (EC). These studies were included in the final synthesis. The synthesized results were subsequently organized in alignment with the research question (RQ) to ensure a clear and comprehensive overview.

3.1. Research on the Application of Blockchain Architecture in Trust Management (Addressing RQ1)

The first research question investigated the function of blockchain technology in preserving the integrity of IoT communication and preventing tampering.. The synthetic results show that the proposed IoT architectures primarily employ permissioned private blockchains (such as Hyperledger Fabric or its variants). Public blockchains, such as Ethereum, cannot meet the requirements for high scalability and low latency when managing a large number of IoT devices. This study highlights three main application areas of blockchain technology. First, there is Device Identity and Access Management (IAM), where smart contracts are used for access authorization. Second, we have Data Integrity Verification, which involves recording sensor data hashes in the ledger to keep things immutable. In conclusion, the non-repudiation mechanism guarantees that once a gateway or device transmits data, it cannot later refute sending the data.

3.2. Quantum Solution Dominance for Cryptographic Key Security (Addressing RQ2)

RQ2 aims to determine which quantum technology solutions are leading in the protection of cryptographic keys on IoT devices. The findings reveal significant differences between quantum key distribution (QKD) and post-quantum cryptography (PQC). QKD is particularly suitable for securing backbone communications, that is, the connection between a central server and resource-

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

intensive IoT gateways. This method is based on the principles of physical security. However, PQC, especially lattice- and hash-based algorithms (such as Kyber and Dilithium), is considered the preferred solution for resource-constrained IoT devices. The analysis shows that while QKD offers higher security, PQC is more practical because of its lower software overhead. Table 1 summarizes the frequency of use of the different PQC algorithms used in this study.

To answer RQ2, we grouped the findings regarding the proposed Quantum Technologies into two main categories: QKD and PQC. Table 1 provides a summary of the qualitative comparison between these two solutions, including their functions, advantages, limitations, and the most prevalent implementation contexts found in the literature.

Our review confirms that Quantum Key Distribution (QKD) [see the first row of Table 2] is considered for use cases where absolute security is paramount, typically at the backbone network layer, where optical hardware can be accommodated. In contrast, the literature indicates that Post-Quantum Cryptography (PQC) dominates proposals for edge devices and IoT end-nodes. In particular, lattice-based PQC algorithms (such as Kyber) are often proposed because of their software-based implementation and lower overhead compared to the complexity of physically installing QKD.

Table 2: Qualitative Comparison of Quantum Technology Implementation in IoT Security (Based on Reviewed Literature)

Technology Category	Key Algorithm/ Schema	Main Functions in IoT	Main Qualitative Advantages (Found in the Study)	Main Qualitative Limitations (Found in the Study	Proposed Implementation
Quantum Key Distribution (QKD	Protokol BB84 MDI-QKD	Physically Secure Authentication and Master Key Distribution	Physically/ Theoretically Guaranteed Security (Based on the Laws of Physics).	Special Optical Infrastructure Requirements, High Costs, Limited Range.	Backbone communication (remote server - gateway)
Post-quantum cryptography (PQC) – lattice-based	Kyber (encryption), Dilithium (Digital Signature)	Session Key Protection and Data Integrity/Device Authentication	*Software-based, Faster Throughput than Physical Quantum, Durable*	*Overhead of Key/Ciphertext Size is Larger, Computational Complexity*.	Edge/End-Node Device (Microcontroller)

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

			against Quantum Attacks.		
Post-Quantum Cryptography (PQC) - Hash-Based	XMSS, SPHINCS+	Quantum-Resistant Digital Signatures	Lightweight Implementation, Well-Proven Security.	Limited Key Usage (Stateful), Slow Signature Computation Time.	Device Authentication with Extremely Limited Resources

3.3. We now discuss the performance challenges and integration trade-offe addressed in RQ3.

In our analysis, we have identified three key trade-offs that arise when attempting to integrate blockchain and quantum technology:

a. Latency is a common issue in blockchain systems, particularly because of the consensus mechanisms that can slow things down, especially at gateways that handle many transactions. Although Permissioned Blockchains offer some improvement in reducing latency compared to Public Blockchains, there is still a significant amount of time involved in block finalization, which remains the biggest obstacle for real-time IoT applications.
b. In the implementation of post-quantum cryptography (PQC) on Internet of Things (IoT) devices, it is crucial to recognize that this generally leads to increased memory consumption and a greater number of CPU cycles than traditional elliptic curve cryptography (ECC) algorithms. Furthermore, the introduction of quantum key distribution (QKD) requires additional investments, including optical infrastructure and key rate management. Interoperability issues: Currently, there is no universal protocol that is accepted for integrating QKD and PQC into the functionality of smart contracts on a blockchain. This causes numerous complex issues in key exchange and lifecycle management.

Discussion

4.1. Let us explore how synergy and the trust framework are integrated in our research.

The findings in the Results section of the report confirm our primary hypothesis that a multilayered approach to trusted communication is imperative in the Internet of Things (IoT). As hypothesized in Research Question 1, the combination of blockchain technology creates a powerful and dependable trust mechanism. This is thanks to decentralized ledgers and smart contracts, which support identity management and ensure data integrity. Therefore, our literature review clearly shows that a layered framework is essential, with blockchain playing a pivotal role in establishing logical trust layers. This layered architectural model generally incorporates several layers, such as an authentication and authorization layer that uses blockchain for identity and access management, a trust management

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

layer that utilizes smart contracts for trust inference and node validation, and a data integrity layer that relies on an immutable, decentralized ledger to ensure data integrity.

Several studies have highlighted the use of clustering approaches in IoT networks that divide the network into zones or clusters, where cluster heads are responsible for conducting local authentication using a private blockchain, while inter-cluster communication uses a global blockchain to maintain the overall security and credibility of the network. This approach facilitates the reduction of latency, enhances scalability, and ensures reliable communications. It is advantageous to consider the integration of blockchain with other technologies, such as edge computing and deep learning, as this combination may provide a more adaptable method for detecting malware and evaluating trust levels in IoT devices. It also helps IoT devices to work better, even though they have limited resources. Smart contracts are important because they can independently handle rules and transactions. This makes things clear and easy to track without the need for outside help. To make this system widely used, we need to solve some major problems. These include large-scale implementation, low energy consumption, and improved interoperability of different IoT platforms.

In addition, the procedure must be simplified. Future research should focus on developing more efficient blockchain protocols, creating energy-efficient consensus mechanisms, and establishing interoperability standards for these systems to improve their performance. These initiatives contribute to establishing a reliable and sustainable IoT ecosystem. Adding blockchain as a trust layer in a multi-layer system for IoT communication helps manage identity, authentication, data integrity, and security policies in a decentralized and secure manner. This method aligns with the initial concept and is supported by the scientific literature. (Abou-Nassar et al., 2020; Honar Pajooh et al., 2021; Kumar & Sharma, 2022; Kokila & Srinivasa Reddy, 2024).

This layer attempts to address the inherent lack of repudiation issues and weaknesses of the traditional Public Key Infrastructure (PKI). In Research Question 2 (FQ2), we attempted to explore the potential for new quantum technologies to add additional layers of security to shield the future from the dangers of quantum computers. This study aims to explain how quantum cryptography and other associated technologies can enhance the safety of existing systems. By utilizing these cutting-edge technologies, we intend to address the issues associated with traditional PKI models, including non-reflection and system inabilities. Post-quantum cryptography (PQC) is paramount in this field and employs cryptographic methods that are resistant to the threat of quantum computers. This is markedly different from older PKI models, such as RSA, DSA, and ECDSA, which are susceptible to quantum computer invasions. PQC employs different approaches, including lattice-based, hash-based, multivariate polynomial-based, and encoding-based cryptographic methods. Its goal is to replace traditional algorithms and ensure persistent protection against potential quantum threats. (Sim 2022; Cherkaoui Dekkaki et al. 2024).

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

We also explore how quantum signatures (QDS) can work with asymmetric quantum keys. This combination allows us to create digital signatures that are not only efficient but also secure from an information-theoretic standpoint.. This means that they ensure integrity, authentication, and non-repudiation while tackling the issues and overheads associated with perfect keys. Modern QDS protocols are impressive; they can operate at high speeds and provide exceptionally strong security, even for very large documents. Plus, they can be practically implemented in quantum networks over distances of hundreds of kilometers, boosting the system's efficiency and resilience against repudiation.(Yin et al., 2023; B.-H. Li et al., 2023).

Furthermore, the issue of a single point of failure, which is a major weakness of the traditional PKI model, can be addressed with a decentralized and distributed approach, allowing for key management and authentication without relying on a single central authority. In this context, blockchain technology and threshold cryptography methods (such as multi-party computation wallets and threshold ECDSA) can support distributed key management, thereby improving security, eliminating single points of failure, and strengthening non-repudiation and data integrity in networks such as vehicle networks or IoT networks.(AlMarshoud et al., 2024a; Benarous et al., 2020)

By combining this layer with quantum and post-quantum technologies, the basic functions of traditional PKI, such as non-repudiation and the authenticity of digital signatures, can be preserved, and security can be improved through resistance to quantum attacks, while addressing vulnerabilities related to critical failure points and system failures that are susceptible to attack. (Cano Aguilera et al., 2024; Yunakovsky et al., 2021). Consequently, this layer provides a solid foundation for the advancement of future secure encryption systems. Crucially, the analysis shows that the synergy between the two technologies is not only additive but also complementary: blockchain manages data trust during transmission, whereas QKD/PQC protects the transmission channel itself.

4.2. Critical Comparison and Implications of Hybrid Solutions

Although the concept of layered security is well established, a review of recent trends regarding hybrid solutions between Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) shows a significant division of roles within the quantum-hybrid security architecture. QKD, which offers theoretical security based on the principles of quantum physics, is best suited for the network backbone, that is, the main communication channels connecting network nodes with high security requirements and direct key exchanges between core users. However, quantum key distribution (QKD) has encountered some limitations, especially in terms of the scalability of authentication and the scope of application, making it less suitable for widely distributed and diverse end devices. On the other hand, post-quantum cryptography (PQC), which is a classically based cryptographic algorithm resistant to quantum computer attacks, offers a viable solution for enhancing communication security, particularly when implemented at the terminal layer. However, while PQC can be effectively utilized on end-node devices because of its

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

ability to provide scalable authentication and compatibility with existing network infrastructure without necessitating specialized hardware, such as single-photon sources, it does not offer the absolute theoretical information security assured by quantum key distribution (QKD) protocols. The combination of these two methods can yield a hybrid solution that integrates QKD into backbone networks and PQC into the end devices. This allows us to fully leverage the advantages of both technologies while overcoming their limitations.

This approach enables the construction of a quantum-resistant communication system, and thanks to QKD technology, it provides a highly secure backbone and scalable authentication and key exchange at the network edges through PQC. Experimental studies and real-world implementations have shown that this method significantly enhances security with acceptable performance trade-offs for practical applications, while also providing resistance to catastrophic cryptographic failures and offering both forward and post-compromise security.(Rubio García et al., 2024; Garms et al., 2024); Yang et al., 2021; Ricci et al., 2024). Thus, a clear division of roles between QKD on the backbone and PQC at the end node represents an important and strategic trade-off in developing practical and scalable quantum communication security solutions for the future. This hybrid approach represents the state-of-the-art direction in quantum-safe communication technology, combining the advantages of quantum physics and quantum-resistant classical algorithms while also providing a modular and adaptive framework for future quantum networks.

Our results highlight that researchers have pragmatically adopted PQC (primarily lattice-based) on resource-constrained devices, accepting greater cryptographic overhead instead of risking a total security failure due to quantum computing. Contrary to previous review studies that solely advocated for Quantum Key Distribution (QKD), the current findings indicate that future trusted communication systems will integrate a range of technologies. These systems do not rely on a single solution; instead, they strategically leverage the strengths of each technology to effectively address a wide spectrum of threats. Future communication systems will be more diverse. To effectively address different threats, we no longer rely on single solutions but employ a combination of technologies to address different threats. This strategy is particularly important in today's communication landscape, especially in scenarios such as smart cities, the Internet of Things (IoT), 6G, connected cars, and satellite networks, which typically involve heterogeneous systems with dispersed technologies and geographical locations.

The following outlines some key points regarding reliable heterogeneous communication architectures and how to address the various threats.

a. Utilizing Various Technologies for Integrated Security: Different communication technologies, such as 5G, IoT, software-defined networking (SDN), edge/fog computing, and non-geostationary satellite technology, each provide their own strengths in dealing with certain types of threats, such as cyberattacks, eavesdropping, data manipulation, and DoS attacks. By building an architecture that collaboratively integrates these various technologies, a more robust and

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

adaptive system against diverse cyber threats can be created.(Akhunzada et al., 2020a; Sung et al., 2016a)

b. Let's talk about how we need to rethink security for future networks like edge and fog computing. These networks are quite distributed and diverse; therefore, sticking to the old, rigid security models will not suffice. Instead, we should move towards a more flexible and collaborative approach. This means creating a security system that can work across different layers and devices, helping us stay aware of potential threats throughout the entire network.(Rapuzzi & Repetto, 2018a).
c. Automatic Adaptation and Artificial Intelligence: Automation of security systems supported by the ability to adapt to a dynamic threat landscape and the use of both external and internal intelligence has become critical. For example, by leveraging SDN's software orchestration capabilities, threats can be proactively and collaboratively addressed, thereby improving the system's responsiveness to various attacks.(Sung et al., 2016b).
d. Physical Layer Security and New Standard Protocols: In communication systems, particularly satellites and wireless networks, physical security approaches such as physical layer security in non-geostationary satellite communications are beginning to receive serious attention to withstand eavesdropping and interference attacks. At the same time, there is a growing need for more secure and integrated communication protocol standards across a variety of heterogeneous services.(Xiao et al., 2019; .Kang et al., 2024)
e. Decentralization and Trust Management: In areas such as vehicular ad hoc networks (VANETs) and the Internet of Vehicles, decentralized models in trust management and authentication reduce single points of failure and enhance system resilience against security threats. Blockchain and threshold cryptography approaches are examples of technologies that support trusted communication architectures in this increasingly heterogeneous future.(AlMarshoud et al., 2024b; Kim et al., 2024).
f. We will examine the adaptability of our model to specific environments, such as intelligent vehicle communications and telematics. In this context, the diversity of protocols and systems may introduce new vulnerabilities to the network. To ensure the security of these networks, a security solution that integrates multiple technologies must be used. This strategy offers layered protection across the application, network, and physical levels.(Y. Li et al., 2019)

In essence, a reliable and diverse communication framework focuses on integrating different communication and security technologies. Each of these technologies addresses specific threats using adaptive, distributed, and multidimensional strategies. This aims to create communication systems that are more robust, resilient, and capable of adapting to the increasingly complex landscape of cyber threats in the future.((Akhunzada et al., 2020b; Rapuzzi & Repetto, 2018b; Sung et al., 2016c; AlMarshoud et al., 2024c).

4.3. Unresolved Challenges and Research Gaps (Future Research Agenda)

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Although the potential for synergy is clear, the performance challenges raised in RQ3, particularly the latency of blockchain consensus and PQC overhead, remain major obstacles to industrial-scale implementation. The latency of blockchain consensus and overhead from Post-Quantum Cryptography (PQC) are the main barriers to industrial-scale adoption. Blockchain consensus, which is a mechanism for reaching an agreement among several nodes in a distributed network, often requires significant computational and communication time, leading to increased transaction latency. This impacts how quickly and efficiently a system can operate, which is particularly important in industrial settings where high speed and scalability are crucial.(Vishwakarma et al., 2022a; Latif et al., 2021)

PQC is all about keeping blockchain technology safe from the potential threats posed by quantum computing. Quantum computers can break the encryption algorithms currently in use. Although post-quantum cryptography (PQC) is crucial for long-term security, it also faces challenges. Algorithms that make them resistant to quantum attacks are generally more complex, requiring more resources for key generation, digital signature creation, and data encryption. (Buser et al., 2023; Fernandez-Carames and Fraga-Lamas, 2020). In the course of evaluating and implementing Post-Quantum Cryptography (PQC) on the Ethereum network under real-world conditions, it has been observed that there is an associated computational overhead. This overhead may impede the processes of transaction and signature verification, consequently affecting the overall efficiency of the system. To mitigate this issue, a feasible solution is to implement more lightweight and efficient consensus mechanisms. For example, the modified Practical Byzantine Fault Tolerance algorithm, or mPBFT, can cut down consensus latency by as much as 90% compared to traditional methods, all without sacrificing performance.(Vishwakarma et al., 2022a). In the domain of post-quantum cryptography (PQC), the employment of hardware acceleration through Graphics Processing Units (GPUs) and Single Instruction, Multiple Data (SIMD) parallelization can decrease the latency and processing overhead of quantum-resistant keys by up to approximately 98% under conditions of low workload. Additionally, it can substantially enhance throughput in scenarios characterized by high workload.(Gao et al., 2022).

The development of quantum-resistant cryptographic methods specifically for blockchain continues, including the use of exotic digital signatures and quantum entanglement-based consensus protocols aimed at balancing strong security and efficiency.(Buser et al., 2023; Qu et al., 2023). Many of these solutions remain in the research or prototype phase and are not yet ready for large-scale industrial implementation or practical applications.

Despite the significant challenges posed by the latency of blockchain consensus mechanisms and the additional complexities introduced by post-quantum cryptography (PQC), extensive research has been conducted in this field. Scholars are striving to develop more efficient consensus algorithms, explore hardware acceleration technologies, and design post-quantum cryptography (PQC) protocols. This study suggests that promising solutions are on the horizon. For large-scale

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

deployments, it is crucial to strike a balance between quantum-resistant security and high-performance requirements. Achieving this equilibrium is essential for ensuring that blockchain systems attain widespread adoption and possess the resilience to withstand future challenges.(Buser et al., 2023); (Vishwakarma et al., 2022b; Gao et al., 2022)

One of the main hurdles is the lack of interoperability standards for managing the lifecycle of keys generated by QKD when using smart contracts on the blockchain. Currently, most research is centered around simulation studies and architectural concepts, with limited evidence of IoT microcontrollers being applied in real-world scenarios, particularly when strict power limits are a concern. Therefore, moving forward, it is important for research to transition from merely exploring concepts to actually testing them in real-life scenarios and developing lightweight end-to-end protocols.

4.4. Methodological Limitations (Acknowledging Limitations)

It is important to note that this SLR has certain limitations. When we limit our search to English-language articles and major scientific databases, we aim to ensure quality; however, this approach might exclude some relevant studies published in regional proceedings or other languages. In addition, because a systematic review is qualitative, our understanding of performance trade-offs relies on the data reported by the authors of the primary studies rather than direct testing. We might be dealing with some reporting bias here; therefore, it is crucial to consider these limitations when interpreting the results of our synthesis.

CONCLUSIONS AND FUTURE WORK

5.1. Conclusions

Through a rigorous Systematic Literature Review (SLR), this study successfully maps and synthesizes the literature regarding the integration of Blockchain and Quantum Technology in realizing Trusted Communication in the Internet of Things (IoT). We confirm that the future architecture of IoT security will be hybrid in nature, utilizing the decentralization of blockchain to ensure non-repudiation and data integrity (RQ1), while also adopting lightweight Post-Quantum Cryptography (PQC) solutions for key security on resource-constrained end-node devices (RQ2). Although there are significant performance trade-offs (particularly consensus latency and PQC overhead), our synthesis supports the perspective that this layered approach is the most promising strategy for addressing existing system vulnerabilities and the threats posed by future quantum computing.

5.2. Future Work

From the gaps highlighted in this review, it appears that there are three main areas where future research could make a difference in bringing Trusted Communication Systems in IoT to life.

First, to better understand how PQC algorithms such as Kyber and Dilithium work on IoT microcontrollers, we need to move beyond simulations. Therefore, real-

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

world implementation studies are essential. These studies will help us measure important factors such as memory overhead, power consumption, and execution time, which are especially critical given the tight power constraints of these devices.

The next step is the standardization of the hybrid protocols. Future efforts should aim to design and test standard protocols that ensure smooth key lifecycle management. This includes integrating the master key distributed by QKD into the authorization and authentication functions of blockchain smart-contract management. Lightweight Consensus Optimization: There Lightweight and more efficient blockchain consensus mechanisms (Lightweight Consensus Mechanisms) that can be applied to IoT gateways to reduce transaction latency and energy bottlenecks without compromising security and immutability must be explored.

REFERENCES

Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O.-Y., Bashir, A. K., & El-Latif, A. A. A. (2020). DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, *8*, 111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468

Akhunzada, A., Islam, S. ul, & Zeadally, S. (2020a). Securing the Cyberspace of Future Smart Cities with 5G Technologies. *IEEE Network*, *34*(4), 336–342. https://doi.org/10.1109/MNET.001.1900559

Akhunzada, A., Islam, S. ul, & Zeadally, S. (2020b). Securing the Cyberspace of Future Smart Cities with 5G Technologies. *IEEE Network*, *34*(4), 336–342. https://doi.org/10.1109/MNET.001.1900559

Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, *16*(23), 10177. https://doi.org/10.3390/su162310177

AlMarshoud, M., Sabir Kiraz, M., & H. Al-Bayatti, A. (2024a). Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. *ACM Computing Surveys*, *56*(10), 1–39. https://doi.org/10.1145/3656166

AlMarshoud, M., Sabir Kiraz, M., & H. Al-Bayatti, A. (2024b). Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. *ACM Computing Surveys*, *56*(10), 1–39. https://doi.org/10.1145/3656166

AlMarshoud, M., Sabir Kiraz, M., & H. Al-Bayatti, A. (2024c). Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. *ACM Computing Surveys*, *56*(10), 1–39. https://doi.org/10.1145/3656166

Benarous, L., Kadri, B., & Bouridane, A. (2020). Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks. *Arabian Journal for Science and Engineering*, *45*(8), 6033–6049. https://doi.org/10.1007/s13369-020-04448-z

Buser, M., Dowsley, R., Esgin, M., Gritti, C., Kasra Kermanshahi, S., Kuchta, V., Legrow, J., Liu, J., Phan, R., Sakzad, A., Steinfeld, R., & Yu, J. (2023). A Survey on

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Exotic Signatures for Post-quantum Blockchain: Challenges and Research Directions. *ACM Computing Surveys*, *55*(12), 1–32. https://doi.org/10.1145/3572771

Cano Aguilera, A., Rubio Garcia, C., Lawo, D., Imaña, J. L., Tafur Monroy, I., & Vegas Olmos, J. J. (2024). In-line rate encrypted links using pre-shared post-quantum keys and data processing units (DPUs). *Scientific Reports*, *14*(1), 21227. https://doi.org/10.1038/s41598-024-71861-x

Chen, Y., Kar, S., & Moura, J. M. F. (2018). Internet of Things: Secure Distributed Inference. *IEEE Signal Processing Magazine*, *35*(5), 64–75. https://doi.org/10.1109/MSP.2018.2842097

Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring Post-Quantum Cryptography: A Review and Directions for the Transition Process. *Technologies*, *12*(12), 241. https://doi.org/10.3390/technologies12120241

Commey, D., Mai, B., Hounsinou, S. G., & Crosby, G. V. (2024). Securing Blockchain-Based IoT Systems: A Review. *IEEE Access*, *12*, 98856–98881. https://doi.org/10.1109/ACCESS.2024.3428490

Diro, A. A., Chilamkurti, N., & Nam, Y. (2018). Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication. *IEEE Access*, *6*, 26820–26830. https://doi.org/10.1109/ACCESS.2018.2822822

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Gao, Y., Xu, J., & Wang, H. (2022). cuNH: Efficient GPU Implementations of Post-Quantum KEM NewHope. *IEEE Transactions on Parallel and Distributed Systems*, *33*(3), 551–568. https://doi.org/10.1109/TPDS.2021.3097277

Garms, L., Paraïso, T. K., Hanley, N., Khalid, A., Rafferty, C., Grant, J., Newman, J., Shields, A. J., Cid, C., & O'Neill, M. (2024). Experimental Integration of Quantum Key Distribution and Postquantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. *Advanced Quantum Technologies*, *7*(4). https://doi.org/10.1002/qute.202300304

Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-Layer Blockchain-Based Security Architecture for Internet of Things. *Sensors*, *21*(3), 772. https://doi.org/10.3390/s21030772

Kang, M., Park, S., & Lee, Y. (2024). A Survey on Satellite Communication System Security. *Sensors*, *24*(9), 2897. https://doi.org/10.3390/s24092897

Kim, M., Oh, I., Yim, K., Sahlabadi, M., & Shukur, Z. (2024). Security of 6G-Enabled Vehicle-to-Everything Communication in Emerging Federated Learning and Blockchain Technologies. *IEEE Access*, *12*, 33972–34001. https://doi.org/10.1109/ACCESS.2023.3348409

Kokila, M., & Srinivasa Reddy, K. (2024). BlockDLO: Blockchain Computing with Deep Learning Orchestration for Secure Data Communication in IoT

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Environment. *IEEE Access*, *12*, 134521–134540. https://doi.org/10.1109/ACCESS.2024.3462735

Kouicem, D. E., Imine, Y., Bouabdallah, A., & Lakhlef, H. (2020). A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/TDSC.2020.3003232

Kumar, R., & Sharma, R. (2022). Leveraging blockchain to ensure trust in IoT: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8599–8622. https://doi.org/10.1016/j.jksuci.2021.09.004

Latif, S., Idrees, Z., Huma, Z., & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey of security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies*, *32*(11). https://doi.org/10.1002/ett.4337

Li, B.-H., Xie, Y.-M., Cao, X.-Y., Li, C.-L., Fu, Y., Yin, H.-L., & Chen, Z.-B. (2023). One-time universal hashing quantum digital signatures without perfect keys. *Physical Review Applied*, *20*(4), 044011. https://doi.org/10.1103/PhysRevApplied.20.044011

Li, Y., Luo, Q., Liu, J., Guo, H., & Kato, N. (2019). TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions. *IEEE Wireless Communications*, *26*(3), 125–131. https://doi.org/10.1109/MWC.2019.1800289

Liu, Y., Hao, X., Ren, W., Xiong, R., Zhu, T., Choo, K.-K. R., & Min, G. (2023). A Blockchain-Based Decentralized, Fair, and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things. *IEEE Transactions on Computers*, *72*(2), 501–512. https://doi.org/10.1109/TC.2022.3157996

Mozzaquatro B. A., Agostinho C., Goncalves D., Martins J., Jardim-Goncalves R. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors*, *18*(9), 3053. https://doi.org/10.3390/s18093053

Muthanna, A., A. Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *Journal of Sensor and Actuator Networks*, *8*(1), 15. https://doi.org/10.3390/jsan8010015

Qu, Z., Zhang, Z., Liu, B., Tiwari, P., Ning, X., & Muhammad, K. (2023). Quantum-detectable Byzantine agreement for distributed data trust management in blockchain. *Information Sciences*, *637*, 118909. https://doi.org/10.1016/j.ins.2023.03.134

Rapuzzi, R., & Repetto, M. (2018a). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. *Future Generation Computer Systems*, *85*, 235–249. https://doi.org/10.1016/j.future.2018.04.007

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Rapuzzi, R., & Repetto, M. (2018b). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. *Future Generation Computer Systems*, *85*, 235–249. https://doi.org/10.1016/j.future.2018.04.007

Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. *IEEE Access*, *12*, 23206–23219. https://doi.org/10.1109/ACCESS.2024.3364520

Rubio García, C., Rommel, S., Takarabt, S., Vegas Olmos, J. J., Guilley, S., Nguyen, P., & Tafur Monroy, I. (2024). Quantum-resistant Transport Layer Security. *Computer Communications*, *213*, 345–358. https://doi.org/10.1016/j.comcom.2023.11.010

Sekaran, R., Patan, R., Raveendran, A., Al-Turjman, F., Ramachandran, M., & Mostarda, L. (2020). Survival Study on Blockchain-Based 6G-Enabled Mobile Edge Computation for IoT Automation. *IEEE Access*, *8*, 143453–143463. https://doi.org/10.1109/ACCESS.2020.3013946

Shim, K.-A. (2022). A Survey on Post-Quantum Public-Key Signature Schemes for Secure Vehicular Communication. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 14025–14042. https://doi.org/10.1109/TITS.2021.3131668

Sung, Y., Sharma, P., Lopez, E., & Park, J. (2016a). FS-OpenSecurity: Taxonomic Modeling of Security Threats in SDN for Future Sustainable Computing. *Sustainability*, *8*(9), 919. https://doi.org/10.3390/su8090919

Sung, Y., Sharma, P., Lopez, E., & Park, J. (2016b). FS-OpenSecurity: Taxonomic Modeling of Security Threats in SDN for Future Sustainable Computing. *Sustainability*, *8*(9), 919. https://doi.org/10.3390/su8090919

Sung, Y., Sharma, P., Lopez, E., & Park, J. (2016c). FS-OpenSecurity: Taxonomic Modeling of Security Threats in SDN for Future Sustainable Computing. *Sustainability*, *8*(9), 919. https://doi.org/10.3390/su8090919

Ullah, F., Salam, A., Amin, F., Khan, I. A., Ahmed, J., Zaib, S. A., & Choi, G. S. (2024). Deep Trust: A Novel Framework for Dynamic Trust and Reputation Management in Internet of Things (IoT)-Based Networks. *IEEE Access*, *12*, 87407–87419. https://doi.org/10.1109/ACCESS.2024.3409273

Vishwakarma, L., Nahar, A., & Das, D. (2022a). LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV. *IEEE Transactions on Vehicular Technology*, *71*(6), 5983–5994. https://doi.org/10.1109/TVT.2022.3163960

Vishwakarma, L., Nahar, A., & Das, D. (2022b). LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV. *IEEE Transactions on Vehicular Technology*, *71*(6), 5983–5994. https://doi.org/10.1109/TVT.2022.3163960

Xiao, Y., Liu, J., Shen, Y., Jiang, X., & Shiratori, N. (2019). Secure Communication in Non-Geostationary Orbit Satellite Systems: A Physical Layer Security

Volume 8 Nomor 3 (2026) 199 – 217 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i3.10819

Perspective. *IEEE Access*, *7*, 3371–3382. https://doi.org/10.1109/ACCESS.2018.2885979

Yang, Y.-H., Li, P.-Y., Ma, S.-Z., Qian, X.-C., Zhang, K.-Y., Wang, L.-J., Zhang, W.-L., Zhou, F., Tang, S.-B., Wang, J.-Y., Yu, Y., Zhang, Q., & Pan, J.-W. (2021). All-optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Optics Express*, *29*(16), 25859. https://doi.org/10.1364/OE.432944

Yin, H.-L., Fu, Y., Li, C.-L., Weng, C.-X., Li, B.-H., Gu, J., Lu, Y.-S., Huang, S., & Chen, Z.-B. (2023). Experimental quantum-secure network with digital signatures and encryption. *National Science Review*, *10*(4). https://doi.org/10.1093/nsr/nwac228

Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., Kiktenko, E. O., Kolycheva, E., Borisov, A., & Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology*, *8*(1), 14. https://doi.org/10.1140/epjqt/s40507-021-00104-z