International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

# A Bibliometric-Based Architectural Framework for Quantum-Safe Low Earth Orbit Satellite Systems

**Muhammad Thafshir Triansha[1], Asep Adang Supriyadi[2], Syachrul Arief[3], Muslimin[4]**

[1,2,3,4] Republic of Indonesia Defense University (UNHAN RI), Bogor, Indonesia

Corresponding Author: mt.thafshir@gmail.com

**Abstract**

*The arrival of practical quantum computing threatens the classical public-key cryptography satellite communication relies on, a threat most acute for Low Earth Orbit (LEO) satellites whose missions span many years. While post-quantum cryptography (PQC) has been studied extensively for terrestrial networks, work bringing it into LEO systems has stayed close to the algorithms and rarely connected to the system-level architecture that must run them under tight resource limits. This study addresses that gap through a bibliometric analysis of 56 Scopus-indexed publications from 2020 to 2026, using keyword co-occurrence and clustering to describe how quantum-secure satellite communication is organized. The analysis identifies four dominant thematic clusters and exposes a structural separation between PQC research and satellite architecture research, sharpest under the constrained conditions of LEO. The study proposes a Resource-Security Co-Design framework uniting lightweight cryptographic control, adaptive authentication, physical-layer entropy reinforcement, and resource-aware orchestration within one architecture, coordinating security and resource management as a single design rather than swapping PQC in as a component. An accompanying feasibility model relates computational complexity, transmission overhead, and onboard resources, setting operational boundaries within which a LEO-class satellite can sustain quantum-safe security. The central contribution is the traceable link between identified gaps and synthesized architecture.*

**Keywords: quantum-safe satellite communication, post-quantum cryptography, LEO satellite systems, cross-layer security architecture, bibliometric analysis, resource-constrained platforms**

## INTRODUCTION

The security of satellite communication has long rested on classical public-key cryptography, with RSA and elliptic curve cryptography (ECC) protecting the confidentiality and integrity of the data exchanged between spacecraft and ground stations (Mosca, 2018; Shor, 1994). The steady maturation of quantum computing now places that foundation in question. A sufficiently capable quantum computer running Shor's algorithm would undo the mathematical assumptions on which RSA and ECC depend, and the consequences are particularly serious for Low Earth Orbit (LEO) satellites that are designed to remain in service for a decade or more. An adversary who records encrypted traffic today can store it and decrypt it later, once the necessary quantum capability becomes available, a strategy commonly described as harvest now and decrypt later. For long-lived space assets this means that information regarded as secure at the moment of transmission may not stay secure across the lifetime of the mission, which is precisely why the move toward quantum-resistant communication has become a pressing concern for the next generation of satellite infrastructure.

Post-quantum cryptography (PQC) has been studied intensively in terrestrial settings, and a substantial body of work now characterizes the performance, key sizes, and security margins of candidate algorithms across a wide range of network conditions (Wang et al., 2026). The situation is far less developed once those same algorithms are carried into orbit. Research on PQC for LEO satellites has remained largely centered on the algorithms in isolation, asking how a given primitive behaves on its own rather than how it fits into the larger system that has to operate it (Qu et al., 2017). This emphasis quietly sets aside a basic operational reality, because LEO platforms work within strict limits on processing power, onboard energy, memory, and available bandwidth (Su et al., 2019), and post-quantum primitives are generally heavier than the classical schemes they are meant to replace, both in the computation they demand and in the size of the keys and signatures they have to transmit. Swapping one algorithm for another, without accounting for the resources that the swap consumes, is therefore unlikely to be sufficient on its own. The harder and more useful question is how quantum-resistant security can be accommodated inside the operational envelope of a small satellite, and that question belongs at the level of system architecture rather than algorithm design alone.

This study approaches the problem by first establishing how the relevant research has actually developed over recent years. It draws on a bibliometric analysis of 56 Scopus-indexed publications appearing between 2020 and 2026, and it applies keyword co-occurrence and clustering to bring the underlying thematic structure of the field into view (Scopus, n.d.). Mapping the literature in this way makes it possible to see which topics tend to be studied

together and which remain apart from one another. The results point to four major research clusters and to a persistent separation between work on PQC algorithms and work on satellite system architecture, a separation that becomes especially clear in studies that have to contend with the resource constraints of LEO operation.

Building on that diagnosis, the study proposes a resource-security co-design paradigm that treats quantum resilience as a property of the whole system rather than the responsibility of a single cryptographic component (Urquhart et al., 2023). The architecture brings together lightweight post-quantum key management, adaptive authentication, physical-layer entropy reinforcement, and resource-aware security orchestration, and it coordinates these functions so that security decisions respond to the operational state of the platform instead of running independently of it. Alongside the architecture, the study develops an analytical feasibility model that traces how computational complexity and transmission overhead relate to the resources a LEO satellite can realistically spare (Wu et al., 2023). The principal contribution is the link itself, the explicit connection drawn between what the bibliometric evidence shows to be missing and an architectural response designed to fill it. What sets the work apart is its framing of quantum-safe satellite security as a resource-constrained optimization problem, one that weighs security and operational cost together within a single design rather than treating them as separate concerns to be settled in turn.

## METHODOLOGY

The study follows a two-stage design. The first stage maps the research landscape through bibliometric analysis, and the second stage translates the resulting findings into an architectural model together with an accompanying feasibility assessment.

### A. Bibliometric Mapping

The first stage examines the research surrounding post-quantum cryptography and satellite communication through a dataset of 56 Scopus-indexed publications published between 2020 and 2026. Article selection followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol, which divides the process into identification, screening, eligibility, and inclusion so that the reason for keeping or discarding each record remains transparent and the search can be reproduced by others (Fernandez-Carames & Fraga-Lamas, 2020; Ralegankar et al., 2022; van Eck & Waltman, 2010). The retained records were then analyzed in VOSviewer using keyword co-occurrence. In this approach two keywords are treated as connected whenever they appear together in the same publication, and the frequency of such joint appearances across the dataset is taken as a measure of how strongly two topics are associated. A minimum occurrence threshold was

applied so that only keywords appearing often enough to be meaningful entered the analysis, which keeps the resulting map readable and reduces the noise that incidental terms would otherwise introduce. Total link strength, defined as the combined weight of all the co-occurrence links attached to a given keyword, was used to gauge how central a term is within the network, and network density was used to describe how tightly the field is connected as a whole.

The purpose of this stage is to make the relationship between PQC algorithm research and satellite system-level architecture research measurable rather than impressionistic. By examining how often the two bodies of work draw on the same vocabulary and settle into the same clusters, the analysis can show where the literature is fragmented and how far existing studies have actually gone toward addressing integration under the resource constraints of Low Earth Orbit.

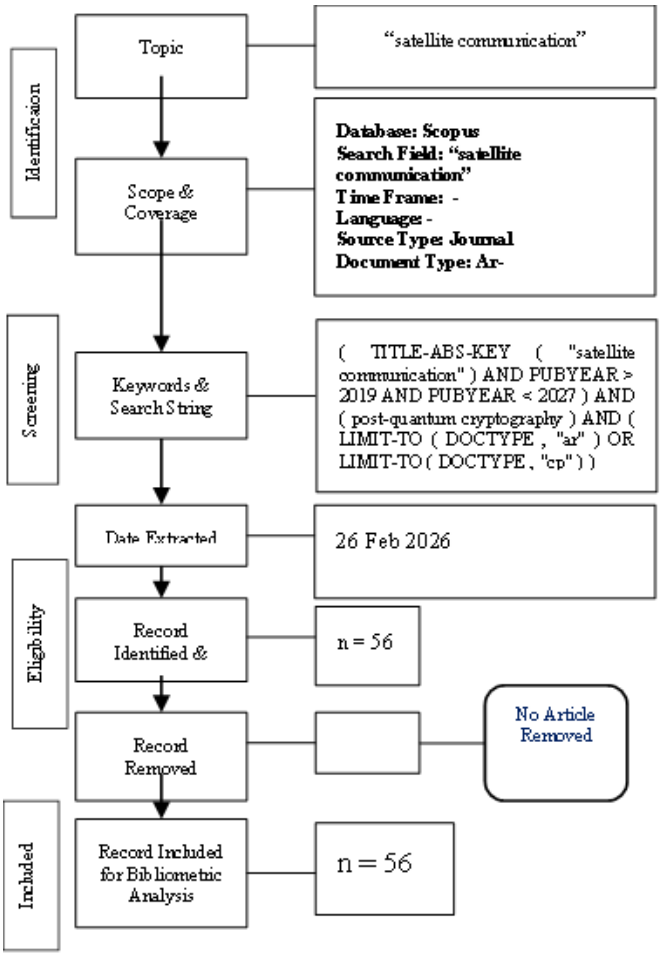



**Figure 1. PRISMA flowchart of the publication selection process.**

### B. Architectural Formulation and Feasibility Modeling

The second stage responds to the structural gap revealed by the mapping. It develops a resource-security co-design architecture organized around cross-layer integration, so that lightweight post-quantum key management, adaptive authentication, physical-layer entropy generation, and resource-aware orchestration operate as parts of one coordinated system rather than as separate additions bolted on after the fact. Designing the architecture in this way allows security requirements and operational resource limits to be weighed together from the very beginning of the design process rather than reconciled at the end.

To test whether the architecture is workable in practice, the study introduces an analytical feasibility model that relates computational cost, transmission overhead, and the resources available on board. The model sets operational boundaries by defining the upper limits of processing complexity and communication load that a LEO platform can sustain, and it provides a quantitative way to judge whether a given quantum-safe mechanism stays within those limits. The value of this stage lies in connecting architectural design to explicit resource constraints, and its originality comes from combining feasibility modeling with cross-layer security design in order to evaluate quantum-safe satellite architectures under the operational limits that genuinely apply in orbit.

## RESULTS AND GAP ANALYSIS

### 2. Bibliometric Network Structure

The keyword co-occurrence analysis produces a dense network organized around the term satellite communication system, which records the highest occurrence frequency and the highest total link strength in the dataset. Its position indicates that this concept functions as the central hub of the field, the point through which several otherwise distinct research areas connect to one another. Applying network-density measures together with the color segmentation that VOSviewer generates, the analysis resolves the network into four major thematic clusters, summarized in Table 1 and discussed in turn in the paragraphs that follow.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

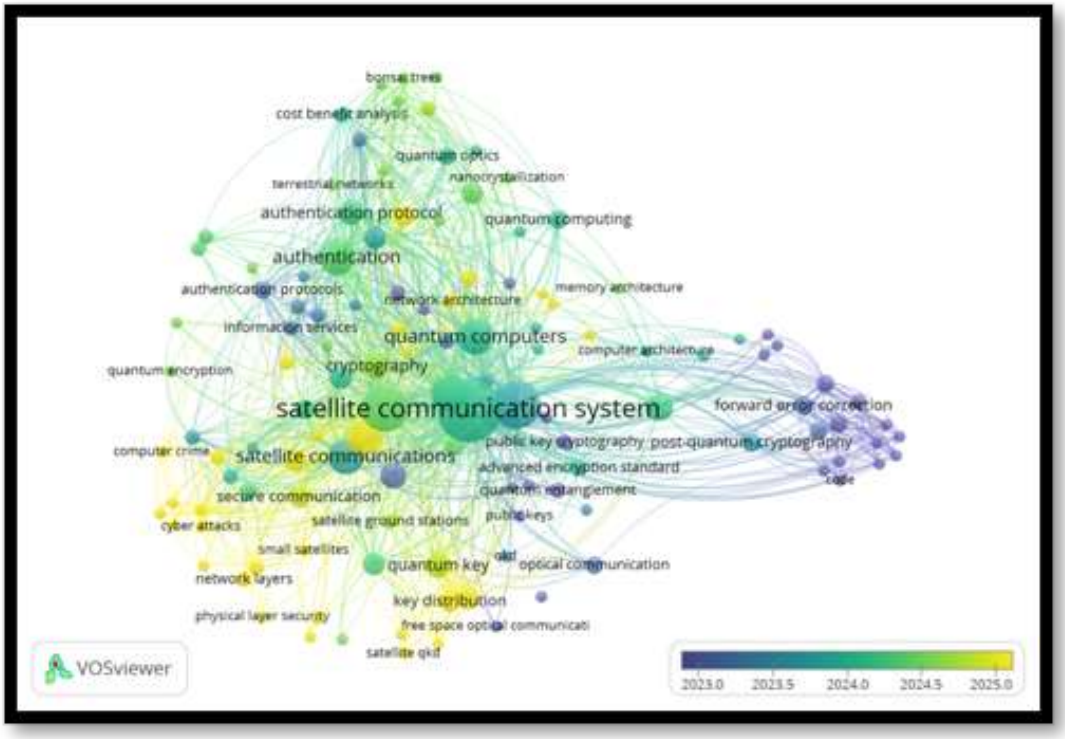



**Figure 2. Overlay visualization of the VOSviewer keyword co-occurrence analysis.**

**Table 1. Thematic clustering results from the keyword co-occurrence analysis (VOSviewer).**

| Cluster | Thematic Label | Dominant Keywords | Research Orientation |
|---|---|---|---|
| C1 | Core Satellite Communication Architecture | satellite communication system, satellite communications, satellite ground stations, small satellites, network layers | System-level communication infrastructure and operational architecture |
| C2 | Quantum Computing and Cryptographic Foundations | quantum computers, quantum computing, cryptography, authentication, authentication protocol, public key cryptography | Algorithmic and theoretical cryptographic development |
| C3 | Post-Quantum Cryptography and | post-quantum cryptography, forward error correction, | PQC resilience and coding-theoretic enhancement |



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

| Cluster | Thematic Label | Dominant Keywords | Research Orientation |
|---|---|---|---|
| | Error Correction | code, advanced encryption standard | |
| C4 | Quantum Key Distribution and Optical Communication | quantum key, QKD, optical communication, quantum entanglement, free-space optical communication | Physical-layer quantum security and optical transmission |

***Interpretation of the Cluster Structure***

The clustering reveals a field that has grown along four largely separate lines, each carrying its own vocabulary and its own internal logic, and each connected only loosely to the others.

The first cluster covers the architecture of satellite communication systems and gathers the core operational building blocks of that architecture, including ground stations, small satellites, and network-layer infrastructure. For all its centrality within the network, this cluster connects only weakly to the post-quantum cryptography themes, which suggests that work on satellite system architecture has so far absorbed very little of the thinking on quantum-resilient security into its own design frameworks.

The second cluster concerns quantum computing and the foundations of cryptography. Its strong internal connectivity reflects a mature and largely self-contained body of theory. The weakness of its links to satellite-related terms, however, indicates that this research usually proceeds without reference to the conditions of an orbital deployment, such as the scarcity of resources and the operational constraints that come with it.

The third cluster brings together post-quantum cryptography and coding techniques. It occupies a partially isolated region of the network, which points to a strong emphasis on algorithmic development. Even where this work engages with forward error correction and coding resilience, it connects only sparingly to research on system-level satellite architecture.

The fourth cluster covers quantum key distribution (QKD) and optical communication, and it leans clearly toward experimental and technological development. Its links to the operational realities of LEO systems, including the computational and energy budgets that such systems impose, remain comparatively thin.

Taken together, the topology describes a clear separation between the architectural, cryptographic, coding, and optical strands of the field. Each one advances along its own track, and there is little sign of the cross-layer integration that any deployable quantum-safe system



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

would ultimately require. This is the central observation that motivates an architecture built to join quantum security to resource management in LEO satellites explicitly rather than by happy accident.

To put this separation on firmer ground, the analysis examines the inter-cluster relationships quantitatively, using total link strength and cross-cluster edge density as reported by VOSviewer. The fragmentation shows up as sparse linkages between the architectural cluster (C1), the cryptographic clusters (C2 and C3), and the optical and QKD cluster (C4), even though cohesion within each individual cluster is high. The scarcity of shared keywords between satellite system architecture and post-quantum cryptography is the clearest empirical signal of this divide, and grounding the observation in measurable network properties keeps the conclusion from resting on interpretation alone.

**B. Structural Fragmentation**

The network shows substantial connectivity inside each cluster and much weaker connectivity between them, a pattern that is consistent with parallel development rather than integrated, system-oriented progress. Four structural gaps follow directly from this pattern.

**G1, Architecture and Cryptography Disconnection.** Research on satellite system architecture (C1) integrates only weakly with post-quantum cryptographic mechanisms (C3), which limits how far quantum-resilient security requirements ever enter the architectural design process in the first place.

**G2, Algorithm-Centric PQC Development.** Work in the PQC domain (C3) concentrates on algorithm design and performance, and comparatively little of it addresses the implementation constraints that a LEO platform imposes.

**G3, Optical and QKD Isolation.** Research on quantum key distribution and optical communication (C4) is oriented toward experimental validation and technological feasibility, and its connection to resource-constrained satellite platforms stays weak.

**G4, Limited Resource-Constrained Modeling.** Across all four clusters, relatively little attention goes to modeling the computational capacity, energy availability, and bandwidth limits that define small-satellite environments.

Together these gaps indicate that quantum-security research for satellite communication has not yet brought security mechanisms, system architecture, and operational resource constraints into a single integrated view.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

### C. Proposed Resource-Security Co-Design Architecture

#### *1) Design Methodology*

The Resource-Security Co-Design (RSCD) framework was developed using Design Science Research (DSR), supported by Model-Based Systems Engineering (MBSE) principles and constraint-driven analytical modeling. Its purpose is to convert the research gaps identified above into a single integrated architecture rather than a loose set of disconnected fixes.

The development proceeded through three stages. The first formalized the structural gaps drawn from the bibliometric analysis. The second decomposed the architecture into layers according to systems-engineering principles. The third produced a feasibility abstraction through resource-constrained modeling, in order to express implementation requirements and operational boundaries in concrete and checkable terms.

Traceability from gap to architecture is the organizing principle throughout the design. Every architectural component is tied back to a specific gap and to the documented limitations in the literature that the gap represents, so that nothing enters the design without an empirical reason for being there.

#### *2) Architectural Structure*

The RSCD framework is built as a cross-layer co-design composed of three coordinated layers that together support quantum-resilient satellite communication.

**a) Physical and Link Support Layer.** This layer supplies entropy reinforcement, awareness of channel state, and forward error correction. These functions sustain reliable communication and strengthen the resilience of the lower layers when operating conditions shift.

**b) Cryptographic Control Layer.** This layer carries the lightweight post-quantum mechanisms, the hybrid classical and PQC transition strategies, and the adaptive authentication functions. It runs the security operations while staying within the implementation limits that satellite platforms impose.

**c) Resource-Aware Orchestration Layer.** This layer watches onboard computation, energy, and bandwidth, and adjusts the security configuration in response, so that what the security layer demands stays matched to what the platform can actually provide.

What sets the RSCD framework apart from a simple cryptographic substitution is that it treats security as a system-level property, one that emerges from the interaction of the architectural layers, the prevailing resource conditions, and the requirements of the specific mission. The contribution is the integration itself, the bringing together of quantum-safe mechanisms, resource management, and architectural coordination inside one design. Its originality lies in making resource-awareness a first-class architectural element of quantum



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

resilient LEO satellite communication rather than an afterthought tacked on once chosen.

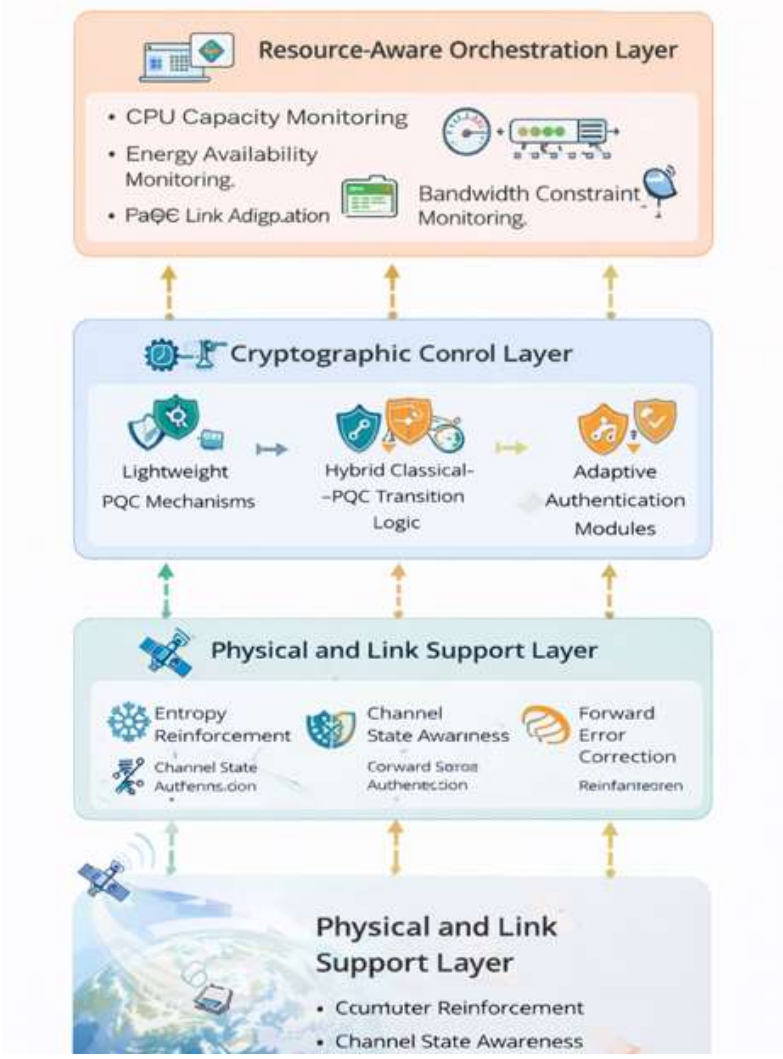



**Figure 3. The RSCD cross-layer co-design framework.**

**Table 2. How the RSCD framework addresses each structural gap.**

| Gap | Architectural Response |
|---|---|
| G1 | Cross-layer coupling between satellite architecture and cryptographic control |
| G2 | Adaptive security selection based on deployment constraints |
| G3 | Integration of physical-layer entropy mechanisms into system-level control |
| G4 | Explicit analytical feasibility modeling under LEO resource bounds |



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

The RSCD framework is derived directly from the gaps that the bibliometric analysis exposed. It does not introduce an architecture invented in the abstract. Instead it turns the observed fragmentation of the field into a coordinated system-level design, gap by gap.

For G1, the disconnection between satellite architecture and post-quantum cryptography, the framework establishes cross-layer coordination between the Physical and Link Support Layer and the Cryptographic Control Layer. Security mechanisms are placed inside the communication architecture rather than bolted on beside it, so that cryptographic functions operate in step with the operational state of the system and with the requirements of the communication layer.

For G2, the algorithm-centric character of PQC development, the Resource-Aware Orchestration Layer allows the security configuration to adapt to the computation, energy, and communication conditions that are actually available at a given moment. A mechanism is then judged not only by its cryptographic strength but by whether a constrained satellite platform can realistically run it.

For G3, the isolation of QKD and optical research, the framework folds entropy reinforcement and channel-state awareness into the system-control process. Physical-layer security properties stop being isolated experimental features and become operational parameters that feed directly into security decisions.

For G4, the limited treatment of resource constraints, the framework formalizes feasibility modeling by treating computational load, energy consumption, and bandwidth use as explicit constraints on the design. Security integration then becomes a constraint-driven synthesis problem rather than a static improvement layered onto an already finished system.

Read as a whole, the mapping shows every component of the RSCD framework answering to a specific gap from the bibliometric study. That correspondence is what ties the empirical diagnosis to the architectural design and gives the framework its analytical footing.

## DISCUSSION

The findings describe a field of quantum-safe satellite communication that is spread across several thematic areas without much contact between them. Post-quantum cryptography, quantum key distribution, and satellite communication systems have each advanced on their own, yet the bibliometric network shows only weak interaction among them. Cohesion runs high inside individual clusters and low across them, and nowhere is the divide sharper than between research on satellite system architecture and research on post-quantum cryptography.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

This fragmentation matters for anyone trying to build a quantum-resilient satellite system. PQC research has concentrated on algorithmic security and mathematical performance, but strength on those measures does not by itself guarantee that an algorithm can run inside a LEO platform. Such platforms are bounded by computation, onboard energy, memory, and bandwidth, and a security mechanism that ignores those bounds is liable to run into trouble the moment it has to operate in orbit.

Research on QKD and optical security shows the same tendency from a different direction. It tends to foreground technological feasibility and experimental validation while saying comparatively little about how these technologies would tie into resource management and adaptive security control. The result is that promising quantum-security techniques remain compartmentalized instead of working as coordinated parts of a single satellite architecture.

The RSCD framework responds to these limitations by treating security as a system-level property shaped by the resources at hand and by the demands of the mission. It joins physical-layer support, cryptographic control, and resource-aware orchestration in one cross-layer structure, an approach that aligns with established systems-engineering practice in its emphasis on requirement traceability, functional integration, and constraint-based design.

The main contribution of this study is to lay out an integration pathway connecting quantum-security mechanisms to satellite resource management. It does not offer new cryptographic primitives. What it offers instead is a disciplined way of moving from empirical bibliometric findings to an architecture, and that route gives the design an evidence base that conceptual architectures assembled without such grounding generally lack.

Some limitations should be stated plainly. The framework is conceptual and rests for now on analytical modeling. The feasibility model marks out operational boundaries under LEO resource constraints, but the study stops short of high-fidelity simulation, hardware prototyping, and in-orbit testing. Later work can carry the framework further through performance evaluation, the development of adaptive orchestration algorithms, and experimental implementation on small-satellite platforms.

## CONCLUSION

This study sets out a conceptual framework for quantum-safe communication in Low Earth Orbit satellite systems, built on a systematic bibliometric gap analysis. The keyword co-occurrence network exposes a structural split among research on satellite architecture, post-quantum cryptography, coding strategies, and quantum-optical security. The weak connectivity across these areas indicates that current work is advancing in parallel rather than coming



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

together within a shared system perspective.

The Resource-Security Co-Design framework answers that fragmentation with a cross-layer integration paradigm that combines cryptographic control, physical-layer reinforcement, and resource-aware orchestration within one coordinated architecture. It treats quantum security as a system-level property governed by the computation, energy, and bandwidth limits that characterize LEO platforms.

The central contribution is a traceable methodological link between empirical bibliometric diagnosis and constraint-driven architectural synthesis. The originality of the work lies in turning documented research fragmentation into a structured set of design principles for integrating quantum-safe security into resource-constrained satellite environments. The framework gives later studies a foundation to build on, whether through quantitative validation, optimization-based orchestration, or experimental deployment on LEO-class satellites.

## ACKNOWLEDGMENT

This research was supported by the National Research and Innovation Agency of Indonesia (BRIN) and the Republic of Indonesia Defense University (UNHAN RI).

## REFERENCES

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

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Qu, Z., Zhang, G., Cao, H., & Xie, J. (2017). LEO satellite constellation for Internet of Things. *IEEE Access, 5*, 18391–18401. https://doi.org/10.1109/ACCESS.2017.2735988

Ralegankar, V. K., et al. (2022). Quantum cryptography-as-a-service for secure UAV communication: Applications, challenges, and case study. *IEEE Access, 10*, 1475–1492. https://doi.org/10.1109/ACCESS.2021.3138753

Scopus. (n.d.). *Scopus indexed journals and metrics*. Elsevier. https://www.scopus.com

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings, Annual IEEE Symposium on Foundations of Computer Science (FOCS)*.

Su, Y., Liu, Y., Zhou, Y., Yuan, J., Cao, H., & Shi, J. (2019). Broadband LEO satellite communications: Architectures and key technologies. *IEEE Wireless Communications, 26*(2), 55–61. https://doi.org/10.1109/MWC.2019.1800299



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Urquhart, J., et al. (2023). A co-design framework for natural resource policy making: Insights from tree health and fisheries in the United Kingdom. *Land Use Policy, 134*. https://doi.org/10.1016/j.landusepol.2023.106901

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics, 84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Wang, S., Du, X., Wu, X., Liu, A., Wang, W., & Cao, Y. (2026). An updatable encryption scheme for blockchain oracle based on post-quantum cryptography. *Cybersecurity, 9*(1). https://doi.org/10.1186/s42400-025-00442-w

Wu, Z., Wang, R., Jia, Z., & Zhu, X. (2023). Simulation modeling methods for LEO satellite communication system. In X. Kong (Ed.), *Proceedings of SPIE: The International Society for Optical Engineering*. SPIE. https://doi.org/10.1117/12.2674971



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.