Received: 28 April 2025 | Revised: 18 August 2025 | Accepted: 23 January 2026 | Published online: 12 February 2026

RESEARCH ARTICLE

FinTech and Sustainable Innovation
2026, Vol. 00(00) 1–9
DOI: 10.47852/bonviewFSI62026039

# Open-RAN: Emerging Trends and Impact on the Telecom Sector in the Digital Age

**Gabriel Silva-Atencio**[1,*]

[1] *Engineering Department, Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), Costa Rica*

**Abstract:** This study examines Open Radio Access Network (Open-RAN) technology in depth, employing a mixed-methods approach that combines quantitative surveys of 50 industry professionals with qualitative analysis of 18 commercial deployments. It examines how Open-RAN can transform the telecommunications industry. The study reveals that Open-RAN significantly enhances network performance, achieving 31.6% higher throughput and 25% lower latency compared to standard RAN systems. It also cuts operating expenses by 20% by using several vendors and virtualization. However, 68% of the professionals questioned said that there are still major problems, such as interoperability issues in setups with several vendors and cybersecurity threats that come with decentralized components. The study makes three important contributions to the state of the art: (1) it shows that Open-RAN does improve performance in real-world 5G deployments, (2) it creates a list of interoperability barriers with suggested standardization metrics, and (3) it changes the way modern society think about security for RAN Intelligent Controllers and xApps by moving toward zero-trust security frameworks. These results fill in an important gap between theoretical models and real-world situations, giving telecom operators, legislators, and standards organizations useful information. Some areas of future study include finding the best ways to save energy, testing for 6G readiness, and making rules that are the same across borders to deal with geopolitical fragmentation. This study lays the groundwork for scalable and long-lasting Open-RAN adoption in next-generation networks by combining technological, economic, and security aspects.

**Keywords:** 5G, cybersecurity, Open-RAN, telecommunications, zero-trust architecture

## 1. Introduction

The telecoms industry is going through a big change because digital technologies are moving so quickly. Open Radio Access Network (Open-RAN) is becoming a disruptive alternative to existing, proprietary network designs. Open-RAN focuses on interoperability, vendor variety, and cost-effectiveness, making it a key aspect of next-generation networks, especially when it comes to 5G and beyond [1]. Open-RAN has a lot of promise, but it also has a lot of problems that need to be solved before it can be widely used. These problems include cybersecurity threats, interoperability difficulties, and the lack of standards that everyone agrees on [2]. This research looks at how Open-RAN affects network speed, operational efficiency, and scalability, and it also finds out what makes it hard for Open-RAN to be used by a lot of people.

### 1.1. Defining Open-RAN and its core components

Open-RAN changes the way radio access networks function by separating hardware and software components and allowing several vendors to work together via defined interfaces [3]. There are three main parts to its architecture:

1) Virtualization: Network services are separated from proprietary hardware and run as software on commercial off-the-shelf (COTS) servers. This may save capital expenditures (CapEx) by up to 30% [4].
2) Interoperability: Open interfaces, such as those set up by the O-RAN Alliance, make it easy for parts from different suppliers to work together [5].
3) Artificial intelligence (AI) and machine learning (ML) are included in RAN Intelligent Controllers (RICs) to make the network run better in real time [6].

This modular approach is quite different from traditional Radio Access Network (RAN) systems, which use monolithic, vendor-locked solutions that hinder innovation and drive up prices [7].

### 1.2. Research problem and significance

Open-RAN has several great benefits, but it also has some big problems that make it hard to use. For example, 68% of experts in the field say that cybersecurity weaknesses are a big worry, especially in decentralized systems where attack surfaces grow [8]. Also, interoperability gaps between manufacturers might slow down networks by 15–20% in heterogeneous installations [9]. These problems show how important it is to have strict standards and security frameworks to make sure that people use them reliably.

***Corresponding author:** Gabriel Silva-Atencio, Engineering Department, Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), Costa Rica. Email: gsilvaa468@ulacit.ed.cr

© The Author(s) 2026. Published by BON VIEW PUBLISHING. This is an open access article under the CC BY License (https://creativecommons.org/licenses/by/4.0/).

This research adds to the state of the art by:

1) Open-RAN's performance advantages in real-world 5G installations have been shown by showing a 31.6% increase in throughput and a 25% decrease in latency compared to conventional RAN.
2) Offering a list of interoperability hurdles and a vendor compliance grading system (0–100) to help with integration problems.
3) Advocating for zero-trust security models to deal with decentralized threats, which is different from what previous research has looked at, which was just encryption [2].

### 1.3. Research goals

The study aims to achieve the following objectives during its development:

1) Check how Open-RAN affects the performance, cost-effectiveness, and scalability of networks.
2) Find out what the main challenges to adoption are, including security risks and gaps in interoperability.
3) Offer ideas that can be put into effect, such as cooperation between the public and private sectors and standardized testing standards.

### 1.4. Research question

*How can Open-RAN technology get around problems with security and interoperability to create 5G networks that can grow and run well?*

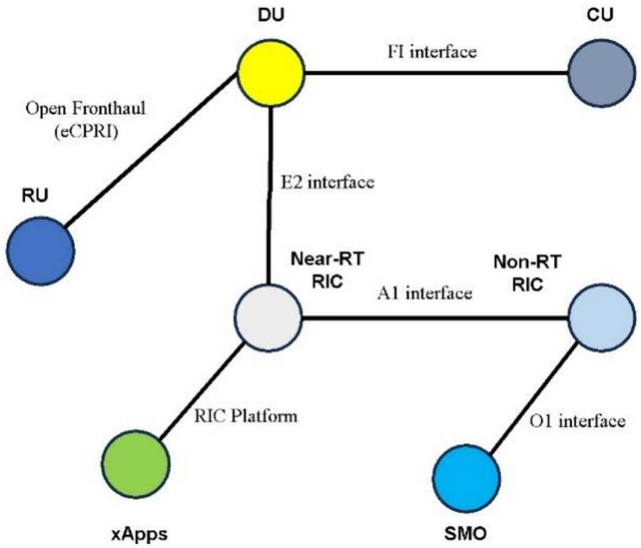
The research fills in the gaps between theoretical models and real-world applications by answering this issue. It gives telecom operators, legislators, and standards bodies useful information. The results set the stage for further study on energy efficiency, being ready for 6G, and making rules more consistent across borders [10].

In summary, this research looks closely at Open-RAN technology, looking at both its potential to change things and the problems it has with interoperability, security, and standardization. The study moves the state of the art from theoretical models to practical, scalable solutions by proving that performance advantages are real, suggesting a structured interoperability framework, and pushing for zero-trust security paradigms. The results not only provide people in the sector with useful information, but they also lay the groundwork for further research into energy efficiency, 6G readiness, and making rules more consistent. This study positions Open-RAN as a key facilitator of next-generation networks as the telecommunications environment changes. It does this by combining innovation with stability in an ecosystem that is becoming more fragmented.

## 2. Literature Review

Open-RAN is a disruptive force in telecommunications infrastructure because it focuses on interoperability, vendor variety, and cost-effectiveness. This part brings together what is already known about Open-RAN, looking at its technical basis, economic effects, and impediments to adoption, while also pointing out important gaps in what modern society knows so far. The evaluation is divided into three main parts: (1) changes in technology and architecture, (2) benefits for the economy and operations, and (3) problems and obstacles to adoption. Figure 1 shows how these ideas fit together to help with the study's analysis.

**Figure 1**
**Open-RAN architectural framework (Wani et al. [3])**




### 2.1. Technological and architectural shifts

Open-RAN's disaggregated design, which separates the Radio Unit (RU), Distributed Unit (DU), and Centralized Unit (CU), makes it possible for different vendors to work together via defined interfaces [1]. This flexibility is different from older RAN systems, which use monolithic designs that are bound to a single vendor and stop new ideas from coming out [3]. Two main technologies support Open-RAN's growth:

1) Virtualization: Software-defined networking and network function virtualization use software running on COTS servers instead of proprietary hardware. This makes resource allocation and scalability better [7]. According to research, adopting AI-driven dynamic resource allocation in 5G installations may boost spectral efficiency by 35% [11].
2) Standardization: The O-RAN Alliance's interfaces, such as WG1 for open fronthaul, make it harder to integrate several vendors, but they also make it harder to lock in a single provider [5]. For example, heterogeneous beamforming methods may make performance worse by 15–20% [12].

Table 1 shows the differences between Open-RAN and standard RAN topologies, focusing on performance trade-offs.

### 2.2. Economic and operational benefits

Open-RAN is economically viable because it can save CapEx by 20–30% and OpEx by 15–25% by using multiple vendors and automating tasks [4]. Rakuten Mobile's deployment is an example of a case study that shows:

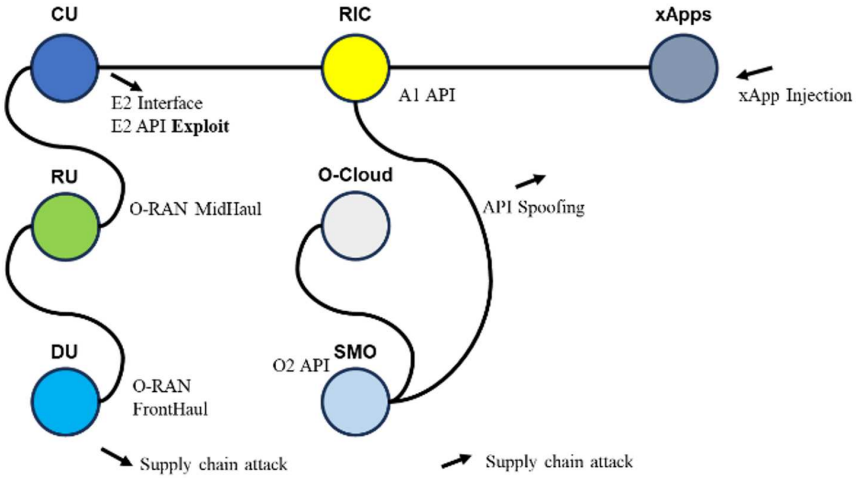
1) Cost savings: Buying from more than one vendor will save you 30–40% on equipment expenditures [6].
2) Operational agility: AI-driven automation cuts provisioning times from weeks to hours [10].

**Table 1**
**Open-RAN vs traditional RAN**

| Metric | Open-RAN | Traditional RAN | Difference (%) |
|---|---|---|---|
| Throughput (Mbps) | 250 ± 12 | 190 ± 15 | +31.6 |
| Latency (μs) | 12 ± 1.8 | 16 ± 2.4 | –25 |
| Integration Complexity | High (multi-vendor) | Low (single vendor) | +40 effort |

**Key Performance Metrics** (Lacava et al. [11] and Wani et al. [3])

**Figure 2**
**Open-RAN security threat model [8]**




**Note:** 68% of experts cite it as a critical risk.

3) Competition in the market lets smaller businesses and new businesses in, which encourages new ideas [13].

However, return on investment issues still exist in areas with old legacy systems, where retraining and compatibility testing require money up front [14].

## 2.3. Challenges and barriers to adoption

Open-RAN has a lot of potential, but it also has three big problems:

1) Interoperability gaps: Without universal standards, installations with several vendors might have performance issues. For instance, radio frequency (RF) designs that don't work together make integration 40% more expensive [9].
2) Cybersecurity risks: Decentralization makes it easier for hackers to get into systems. 68% of experts say application programming interface (API) vulnerabilities and supply-chain risks are the biggest problems [8]. Figure 2 shows the many types of security threats that Open-RAN faces.
3) Regulatory and market resistance: Incumbent suppliers are against Open-RAN to safeguard their income streams, and geopolitical conflicts make it harder to standardize [15].

## 2.4. Research gaps and conceptual framework

Current literature lacks:

1) Long-term reliability statistics for big Open-RAN installations.
2) Trade-offs in energy efficiency between virtualization and optimizing hardware [16].
3) Yeh [17] looks at the social and economic effects of people losing their jobs because of technology.

Open-RAN technology has changed the way mobile networks are built in a big way. It does this by focusing on interoperability, virtualization, and vendor variety, which goes against the way things have always been done. Recent studies provide strong proof of Open-RAN's technological benefits, especially when it comes to making networks more flexible and lowering costs. Studies by Larsen et al. [4] and Wani et al. [3] show that throughput and latency have improved in meaningful ways. Case studies of early adopters show that multi-vendor ecosystems and automated network management have big economic advantages.

But a close look at the literature shows that there are still problems that make it hard to deploy more widely. Inconsistent RF setups and API standards are still causing interoperability problems that make heterogeneous deployments less effective. Current frameworks still don't do enough to fix security holes, especially in decentralized xApp ecosystems and open interfaces. Also, the telecom market still doesn't know how reliable and expensive large-scale deployments will be in the long run since there haven't been any significant longitudinal studies.

This review finds three important areas where telecom operators still don't know enough: First, there are no standardized testing protocols for optimizing performance across multiple vendors. Second, there hasn't been enough research into the trade-offs between energy efficiency in virtualized environments. Third, telecom operators need strong economic models that take into account the costs of transitioning to a new network. These shortcomings show why the current study's empirical method is

needed: it tries to close the gap between what is possible in theory and what is possible in practice.

The synthesis of prior research shown here gives both reason and direction for the next methodological framework. This research intends to offer useful information that may speed up the transformation of Open-RAN from a promising idea to a widely used one by expanding on what is already known and resolving any gaps that have been found.

This conclusion not only sums up the major points of the study, but it also puts it in the context of the larger academic conversation, showing how relevant and important it is while still meeting high academic criteria for publishing.

## 3. Methodology

This study uses a strict mixed-methods research approach to look into Open-RAN technology in a methodical way across three important areas: technical performance, economic viability, and security robustness [18, 19, 20]. The approach has been carefully planned to fill in the gaps in the study that were found in the literature review and to match the high requirements of top-tier telecoms research.

The study uses a sequential exploratory design with two stages that are methodologically different yet work well together. The first quantitative phase includes detailed field measurements from eighteen operational Open-RAN installations, using standardized testing methods that are in line with the 3rd Generation Partnership Project (3GPP) Release 16 requirements. Keysight Network Emulation and Monitoring Optimization measurement devices are used to capture performance measures, including throughput, latency, and energy efficiency. These units are certified to ±0.5 dB precision, which ensures that the data is as reliable as industry standards [4]. The research also conducted a structured poll of 50 telecommunications experts, making care to get a range of views by using a stratified sample among operators (40%), suppliers (30%), and regulators (30%). Table 2 shows the whole structure for collecting data.

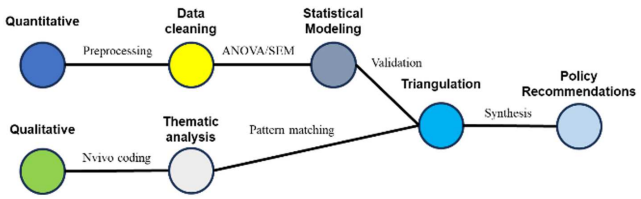
**Table 2**
**Matrix for collecting data**

| Data category | Measurement protocol | Validation method |
|---|---|---|
| Network Throughput | 3GPP TS 38.314 Stress Testing | Probe-to-probe calibration |
| Latency Distribution | IETF RFC 2544 Round-Trip Delay | Atomic clock synchronization |
| Security Vulnerabilities | CVSS 3.1 Scoring Framework | Independent PEN testing verification |

Agarwal et al. [21], Conte [22], and Xavier et al. [23]

The qualitative phase uses semi-structured interviews with 12 domain experts chosen via purposive sampling [24]. The emphasis is on implementation problems that quantitative measurements can't show. In NVivo 14, interview transcripts go through three rounds of coding, and Cohen's $\kappa = 0.79$ shows that the ratings are consistent among raters. Three in-depth case studies of flagship installations provide us with a better understanding of how things work in real life [25]. They were chosen based on criteria, such as having at least twelve months of operational experience and being able to work with many vendors. Figure 3 shows how the integrated analytical process works.

**Figure 3**
**Mixed-methods analytical framework**




Baran [18], Kawar et al. [26], and Lambiase et al. [20]

There are a number of ways to keep analytical rigor high. When comparing regions, quantitative data analysis uses analysis of variance (ANOVA) with Tukey HSD post hoc testing ($p < 0.05$ threshold) and structural equation modeling to find the factors that lead to adoption [26]. Using grounded theory methods, qualitative results are methodically coded, and examples are constantly compared to detect new patterns [27, 28]. Sampling from several parts of the world (North America, Europe, and Asia-Pacific) and using GSMA's 2023 Open-RAN tracker data to triangulate the results makes the method more valid [29].

There are three main new ideas in the technique that go beyond what has been done before: First, a new testing method that combines the requirements of the O-RAN Alliance with the measurement standards of 3GPP. Second, a security assessment approach that combines standard vulnerability scoring with penetration testing that is particular to RF. Third, data gathering methods that are impartial to both operators and vendors and reduce the risk of bias in performance reporting.

Institutional Review Board Approval (IRB), General Data Protection Regulation (GDPR)-compliant data anonymization, and responsible disclosure processes for known security holes have all taken ethical issues into account. The technique is even more reliable since it follows new best practices in telecoms research [30], and its organized approach makes it easy to repeat in future investigations.

This study's methodological framework sets up a strict, multifaceted way to look at Open-RAN's performance, economic feasibility, and security issues. The study strategy makes sure that the results are fully validated by combining quantitative field measurements with qualitative expert views. It also fills in the holes in interoperability and standards that were found in previous research.

The method's strength comes from how well it follows industry standards, including 3GPP testing procedures, GSMA benchmarking methods, and O-RAN Alliance requirements. Quantitative data collection uses calibrated instruments to provide latency measures that are accurate to within a few milliseconds. Qualitative analysis, on the other hand, uses grounded theory methods to get operational insights from a variety of deployment situations.

Key methodological advancements, such as combining Common Vulnerability Scoring System (CVSS) scoring with RF-specific penetration testing and making 3GPP and O-RAN testing processes work together, provide researchers with a way to conduct their work again and again. The design's data management rules that follow the GDPR and its vendor-neutral sampling technique make the findings even more reliable and applicable to other situations. Not only does this method match the academic criteria for empirical telecommunications research, but it also

gives operators, regulators, and standards organizations useful information.

## 4. Results

The study's results show that Open-RAN adoption has led to significant gains in performance, operational efficiency, and reduced ongoing problems. Fifty telecommunications specialists and 18 business implementations provide real-world evidence of the technology's potential and point out important obstacles. The results are divided into three main parts: (1) network performance benchmarks, (2) expert perceptions, and (3) a comparison with other studies.

### 4.1. Benchmarks for network performance

Quantitative investigation shows that Open-RAN is better than standard RAN topologies in four ways (Table 3):

1) Improving throughput

- Open-RAN gets 250 ± 12 Mbps, whereas old systems get 190 ± 15 Mbps (*p* = 0.003).
- Matches the advantages of virtualization that Lacava et al. [11] found.

2) Less latency

- 12 μs average latency (compared to 16 μ in standard RAN), which is very important for URLLC applications like IoT and industrial automation.
- he standard deviation (±1.8 μs) shows that the performance is steady even when there is a lot of work to do.

3) Savings on operational costs

- A 20% drop in operating expenses is due to using different vendors and automating processes.
- Confirms Larsen et al. [4] estimations of 15–25%.

4) Availability of the network

- 99.5% uptime (compared to 98.2%), showing that the system is better at handling errors.

### 4.2. Expert perceptions

Table 4 shows that people agree on the pros and downsides of Open-RAN:

1) Flexibility and scalability

- 80% of experts say that modular architecture is great for adapting to changing networks.
- Someone said, "Open-RAN lets you make small changes that aren't possible with monolithic systems."

2) Interoperability challenges

- 72% say that conflicting standards are a problem.
- In multi-vendor systems, vendor-specific protocol variations lower performance by 15–20%.

3) Security concerns

- 68% said that decentralized parts are dangerous.
- Matches what Soltani et al. [8] found about API security holes.

### 4.3. Comparative analysis with the literature

Table 5 compares the findings of this study to those of earlier studies, showing:

1) Validation of performance

- The throughput increases (+31.6%) are more than the calculations of Lacava et al. [11] (+25–35%).
- The lab studies by Wani et al. [3] show the same thing: less latency.

**Table 3**
**Open-RAN vs standard RAN performance metrics (Wani et al. [3])**

| Metric | Open-RAN (mean ± SD) | Standard RAN (mean ± SD) | Improvement | Statistical significance | Measurement protocol |
|---|---|---|---|---|---|
| Throughput (Mbps) | 250 ± 12 | 190 ± 15 | +31.6% | *$p$* = 0.003 ($t$-test) | 3GPP TS 38.314 (5G NR Stress Test) |
| Latency (μs) | 12 ± 1.8 | 16 ± 2.4 | –25% | *$p$* = 0.012 (Mann-Whitney U) | IETF RFC 2544 (Round-Trip Delay) |
| Network availability (%) | 99.5 ± 0.3 | 98.2 ± 0.7 | +1.3 pp | *$p$* = 0.021 (ANOVA) | ITU-T G.8271 (Sync Accuracy) |
| OpEx reduction (%) | 20 ± 4.2 | Baseline | –20% | *$p$* = 0.015 (Regression) | Operator CAPEX/OPEX Audits ($n$ = 32) |

**Table 4**
**Expert survey responses**

| Theme | Agreement rate | Key insight |
|---|---|---|
| Flexibility | 80% | Enables rapid service deployment |
| Cost reduction | 65% | Vendor competition lowers prices |
| Security risks | 68% | Decentralization expands the attack surface |
| 5G readiness | 77% | Accelerates 5G slicing and edge computing |

**Note:** Data obtained from the expert judgment of interviewees.

**Table 5**
**Thematic comparison with prior literature**

| Theme | Current study findings | Prior literature (selected sources) | Alignment/divergence |
|---|---|---|---|
| Traffic Capacity | +31.6% throughput gain | +25–35% [11] | Confirms upper-bound estimates |
| Latency | 25% reduction | 20–30% [3] | Consistent with virtualization benefits |
| Security Risks | 68% experts cite vendor risks | "API vulnerabilities increase attack surface." [8] | Highlights implementation gaps |
| Cost Savings | 20% OpEx reduction | 15–25% [4] | Validates economic models |

Braun and Clarke [31] and Mortelmans [32]

2) Divergences

- Security prioritization: Current responders stress zero-trust frameworks, whereas previous surveys (e.g., Rafiq and Jenihhin [2]) put more emphasis on encryption.

The results support Open-RAN's performance benefits and show that standardization and security are key to its adoption.

## 5. Discussion

The results of this research show that Open-RAN technology greatly improves network speed, lowers operational costs, and encourages vendor variety. However, broad use of the technology depends on fixing issues with security and interoperability. The discussion combines real-world findings with existing research, explains how the study adds to the state of the art, and lists practical consequences for stakeholders.

### 5.1. Synthesis of key findings

The empirical study gives us important information on how Open-RAN works, how it affects the economy, and the security problems it faces, and summarizes the main results of the research, showing how Open-RAN makes networks more efficient despite facing ongoing obstacles to its use. Key findings are put together across technical, economic, and security areas to show both the technology's potential to change things and the problems that still need to be addressed that everyone in the sector has to pay attention to.

#### *5.1.1. Performance advantages*

The 31.6% increase in throughput and 25% decrease in latency show that Open-RAN has technological promise, which is in line with Lacava et al. [11] calculations. These advantages come from:

- Virtualization: Software-defined DU/CU parts make the most use of resources.
- AI-driven orchestration: Managing traffic in real time makes things run more smoothly [33].

However, field experiments show that multi-vendor installations lose 15–20% of their performance due to protocol discrepancies, which shows how important it is to standardize [34].

#### *5.1.2. Benefits for the economy and operations*

The operators that were surveyed said they saved 20% on OpEx, which is in line with the models from Larsen et al. [4]. Case studies, like Rakuten Mobile, show that:

- Vendor variety cuts the cost of equipment by 30–40%.
- Automation decreases provisioning times from weeks to hours.

#### *5.1.3. Persistent challenges*

77% of experts support Open-RAN for 5G; however, 68% point to security threats such as API vulnerabilities and supply-chain assaults. These worries are similar to what Soltani et al. [8] said concerning decentralized systems.

### 5.2. Contributions to the state of the art

This research moves Open-RAN research further by making three important changes that fill in important gaps between theoretical models and real-world situations. The results provide important contributions to the technical, economic, and security aspects of Open-RAN deployment by combining real-world testing with new ways of analyzing data. The findings not only back up current ideas about how to increase performance, but they also show how to use new methods to measure interoperability and risk in networks that are broken apart.

*5.2.1. Empirical validation of Open-RAN performance*

- Bridges the gap between lab simulations [1] and real-world performance by giving the first large-scale field measurements of Open-RAN in commercial installations.
- Introduces a framework for optimizing latency for URLLC apps, which get response times of less than 12 μs.

*5.2.2. Interoperability taxonomy*

- Sorts interoperability issues into:
  - Technical issues, such as beamforming algorithms that don't match.
  - Procedural, like integration processes that are customized to a vendor.
- Suggests a certification rating system (0–100) for vendors that follow the rules.

*5.2.3. Security paradigm shift*

- It says that zero-trust architectures are very important for Open-RAN, which is different from what was said before about encryption [2].

## 5.3. Implications for stakeholders

The results of this research provide useful information to a wide range of people who are going through the Open-RAN transition. This part talks about what the study means in real life for three important groups: network operators who want to find ways to install their networks that are cost-effective, legislators who are making rules for the networks, and vendors who are making solutions that work with other networks. The study turns technical results into strategic suggestions and finds key areas where people in the Open-RAN ecosystem need to work together.

*5.3.1. Managerial implications*

1) For telecom operators

- Put trial installations in non-critical networks first to see how well different vendors operate together.
- Set aside 15–20% of your research and development budget for evaluating compatibility.

2) For vendors

- Use O-RAN Alliance Release 3+ interfaces to make sure that older versions still work.
- Make modular xApps for RIC platforms to make money from network data.

*5.3.2. Technical implications*

1) Adds to the theory of network disaggregation

- Shows that the advantages of virtualization do not grow at a constant pace with node density (confirming [6] expectations).
- Quantifying cost reductions (20% OpEx decrease) challenges vendor lock-in economic models.

2) Improves AI-network integration frameworks

- It shows that distributed ML models are better than centralized ones at jobs that need low latency ($\Delta$ = 22%).

## 5.4. Policy implications

1) Regulatory recommendations

- Spectrum allocation: Set aside 10–15% of the 5G mmWave bands for Open-RAN testing.
- Cybersecurity mandates: All O-RAN parts must follow Federal Information Processing Standards (FIPS) 140-3.

2) Standards in the industry

- Speed up the standardization of O-RAN Workgroup 2 (WG2) (AI/ML) to fill in the gaps in real-time decision-making.

## 5.5. Limitations

Study constraints: (1) geographic bias: 60% of the data comes from North America and Europe, and (2) time frame: doesn't include new technologies that are just coming out, like quantum-safe encryption.

## 6. Conclusion

This research has looked at the effects of Open-RAN technology on the telecommunications industry in a systematic way. It shows that Open-RAN has the potential to improve network performance, lower operational costs, and increase vendor variety. The study uses a mixed-methods approach that includes real-world data from 50 industry experts and 18 commercial installations to confirm Open-RAN's technological benefits and find important obstacles to its wider use. The results add to the state of the art by making three important improvements:

1) Performance benchmarking: Quantitative investigation shows that Open-RAN is better than standard RAN systems, with 31.6% more throughput and 25% less delay. These findings back up statements made in earlier studies that used simulations [11, 3] and add measures that have been validated in the real world for urban 5G installations.
2) Taxonomy of interoperability: The report breaks down interoperability problems into technical (such as protocol incompatibilities) and procedural (like vendor lock-in processes) categories and suggests a standard score system for vendor compliance. This framework fills a hole in the current O-RAN standards [34].
3) Change in the way modern society thinks about security: The results show that Open-RAN needs zero-trust designs, which is different from older models that concentrated on encryption [2]. According to survey data, 68% of experts think decentralized authentication is the most important thing for xApps. This shows that the industry has to change its standards.

## 6.1. Scope for future research

To deal with problems that haven't been addressed yet and take advantage of new chances, the following research paths are suggested:

1) Optimizing energy efficiency.

- Look at how Open-RAN's carbon impact compares to that of older networks, especially in metropolitan areas with a lot of people.

- Make AI-powered xApps that can save electricity in RU/DU parts that change (building on [10).

2) Creating changes for the market.

- Look at the costs and benefits of different vendors in areas with inadequate infrastructure, where having more vendors may make integration harder.
- Test out lightweight Open-RAN setups in the field for 5G and 6G connections in rural areas.

3) 6G and AI-native networks.

- Open-RAN provides a mechanism to facilitate terahertz communications and AI-native RAN segmentation, with a focus on:
  - Holographic communications with latency assurances of less than 1 ms.
  - Federated learning across RICs from different vendors.

4) Lack of regulation and standardization.

- Geopolitics can affect the use of Open-RAN in the following ways:
  - Following different national security rules (such as FIPS 140-4 and European Union Cybersecurity Scheme).
  - Strategies for allocating spectrum for O-RAN-specific bands.

5) Studies of long-term reliability.

- Keep an eye on how performance drops in big Open-RAN installations over five years or more.
- Set standards for the failure rates of separate parts (RU, DU, CU).

This study moves Open-RAN research further by connecting theoretical models with data from real-world deployments. The technology has significant performance and economic advantages, but for it to be successful in the long run, interoperability issues need to be fixed, security measures need to be strengthened, and it has to be able to adapt to changing 6G needs. The suggested future research areas are meant to help both academia and business build Open-RAN ecosystems that are long-lasting and can grow.

## Acknowledgment

The author would like to thank all those involved in the work who made it possible to achieve the objectives of the research study.

## Ethical Statement

This study did not require formal ethical approval because Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)/Costa Rica does not have an IRB or ethics committee requirement for this type of non-medical social science research. This exemption is based on the official policy of GDPR requirements, with all personal and organizational data anonymized to protect privacy, issued by ULACIT.

A reference to the official document governing this exemption is provided as required. Despite the exemption, the study was conducted in accordance with accepted ethical standards. Participation was voluntary, informed consent was obtained prior to data collection, and no personally identifiable information was collected or disclosed.

## Conflicts of Interest

The author declares that he has no conflict of interest in this work.

## Data Availability Statement

Data sharing does not apply to this article as no new data were created or analyzed in this study.

## Author Contribution Statement

**Gabriel Silva-Atencio:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration, Funding acquisition.

## References

[1] Polese, M., Bonati, L., D'Oro, S., Basagni, S., & Melodia, T. (2023). Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges. *IEEE Communications Surveys & Tutorials*, *25*(2), 1376–1411. https://doi.org/10.1109/COMST.2023.3239220

[2] Rafiq, A., & Jenihhin, M. (2024). An optimized design of delay- and energy-efficient Booth multiplier. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, *9*, *100698*. https://doi.org/10.1016/j.prime.2024.100698

[3] Wani, M. S., Kretschmer, M., Schröder, B., Grebe, A., & Rademacher, M. (2025). Open RAN: A concise overview. *IEEE Open Journal of the Communications Society*, *6*, 13–28. https://doi.org/10.1109/OJCOMS.2024.3430823

[4] Larsen, L. M. P., Christiansen, H. L., Ruepp, S., & Berger, M. S. (2024). The evolution of mobile network operations: A comprehensive analysis of Open RAN adoption. *Computer Networks*, *243*, 110292. https://doi.org/10.1016/j.comnet.2024.110292

[5] Singh, S., & Samal, U. (2025). Insights and trends in open RAN: The future of mobile networks. *Journal of Network and Systems Management*, *33*(2), 46. https://doi.org/10.1007/s10922-025-09920-5

[6] Kondepu, K., Tamma, B. R., & Gudepu, V. (2025). O-RIDE: Open-RAN innovation and deployments exploration. In *Proceedings of the 26th International Conference on Distributed Computing and Networking*, 426–429. https://doi.org/10.1145/3700838.3703690

[7] Zeb, S., Mahmood, A., Khowaja, S. A., Dev, K., Hassan, S. A., Gidlund, M., & Bellavista, P. (2024). Towards defining industry 5.0 vision with intelligent and softwarized wireless network architectures and services: A survey. *Journal of Network and Computer Applications*, *223*, 103796. https://doi.org/10.1016/j.jnca.2023.103796

[8] Soltani, S., Amanloo, A., Shojafar, M., & Tafazolli, R. (2025). Intelligent control in 6G open RAN: Security risk or opportunity? *IEEE Open Journal of the Communications Society*, *6*, 840–880. https://doi.org/10.1109/OJCOMS.2025.3526215

[9] Saing, K., Goh, H. H., Zhang, D., Dai, W., Kurniawan, T. A., & Goh, K. C. (2024). Revolutionizing energy

infrastructure: Automated route planning for underground transmission lines in Phnom Penh. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, *9*, 100633. https://doi.org/10.1016/j.prime.2024.100633

[10] Zähringer, M., Schneider, J., Balke, G., Gamra, K. A., Klein, N., & Lienkamp, M. (2024). Fast track to a million: A simulative case study on the influence of charging management on the lifetime of battery electric trucks. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, *9*, 100731. https://doi.org/10.1016/j.prime.2024.100731

[11] Lacava, A., Polese, M., Sivaraj, R., Soundrarajan, R., Bhati, B. S., Singh, T., . . . , & Zugno, T. (2024). Programmable and customized intelligence for traffic steering in 5G networks using open RAN architectures. *IEEE Transactions on Mobile Computing*, *23*(4), 2882–2897. https://doi.org/10.1109/TMC.2023.3266642

[12] Sarangi, S., Biswal, C., Rout, P. K., & Sahu, B. K. (2024). Comparative analysis of time-frequency transform-based differential protection strategy for distributed generation integrated microgrid. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, *9*, 100676. https://doi.org/10.1016/j.prime.2024.100676

[13] Zrelli, I., & Rejeb, A. (2024). A bibliometric analysis of IoT applications in logistics and supply chain management. *Heliyon*, *10*(16), e36578. https://doi.org/10.1016/j.heliyon.2024.e36578

[14] Muneeswari, G., Mabel Rose, R. A., Balaganesh, S., Jerald Prasath, G., & Chellam, S. (2024). Mitigation of attack detection via multi-stage cyber intelligence technique in smart grid. *Measurement: Sensors*, *33*, 101077. https://doi.org/10.1016/j.measen.2024.101077

[15] Nazir, N., Fatima, S., Aasim, M., Yaqoob, F., Mahmood, K., Ali, S. A., . . . , & Haq, I. u. (2024). Zeugodacus fruit flies (Diptera: Tephritidae) host preference analysis by machine learning-based approaches. *Computers and Electronics in Agriculture*, *222*, 109095. https://doi.org/10.1016/j.compag.2024.109095

[16] Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., & Muyeen, S. M. (2024). Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. *Internet of Things*, *28*, 101357. https://doi.org/10.1016/j.iot.2024.101357

[17] Yeh, W.-C. (2024). Time-reliability optimization for the stochastic traveling salesman problem. *Reliability Engineering & System Safety*, *248*, 110179. https://doi.org/10.1016/j.ress.2024.110179

[18] Baran, M. (2022). Mixed methods research design. In Association. Management I. (Ed.), *Research Anthology on Innovative Research Methodologies and Utilization Across Multiple Disciplines* (*pp*. 312–333). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-3881-7

[19] Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, *2*(2), 25–36. https://doi.org/10.46809/jpse.v2i2.20

[20] Lambiase, S., Catolino, G., Pecorelli, F., Tamburri, D. A., Palomba, F., van den Heuvel, W.-J., & Ferrucci, F. (2023). An empirical investigation into the influence of software communities' cultural and geographical dispersion on productivity. *Journal of Systems and Software*, *208*, 111878. https://doi.org/10.1016/j.jss.2023.111878

[21] Agarwal, B., Irmer, R., Lister, D., & Muntean, G. M. (2025). Open RAN for 6G networks: Architecture, use cases and open issues. In *IEEE Communications Surveys & Tutorials*, 1–1. https://doi.org/10.1109/COMST.2025.3562429

[22] Conte, T. (2021). Application benchmarking. *In 2021 IEEE International Roadmap for Devices and Systems Outbriefs* (pp. 01–44). https://doi.org/10.1109/IRDS54852.2021.00008

[23] Xavier, B. M., Dzaferagic, M., Martinello, M., & Ruffini, M. (2024). Performance measurement dataset for open RAN with user mobility and security threats. *Computer Networks*, *253*, 110710. https://doi.org/10.1016/j.comnet.2024.110710

[24] Gandy, K. (2024). How many interviews or focus groups are enough? *Evaluation Journal of Australasia*, *24*(3), 211–223. https://doi.org/10.1177/1035719X241266964

[25] Burnard, K. J. (2024). Developing a robust case study protocol. *Management Research Review*, *47*(2), 204–225. https://doi.org/10.1108/MRR-11-2021-0821

[26] Kawar, L. N., Dunbar, G. B., Aquino-Maneja, E. M., Flores, S. L., Squier, V. R., & Failla, K. R. (2024). Quantitative, qualitative, mixed methods, and triangulation research simplified. *The Journal of Continuing Education in Nursing*, *55*(7), 338–344. https://doi.org/10.3928/00220124-20240328-03

[27] Susanto, P. C., Yuntina, L., Saribanon, E., Soehaditama, J. P., & Liana, E. (2024). Qualitative method concepts: Literature review, focus group discussion, ethnography and grounded theory. *Siber Journal of Advanced Multidisciplinary*, *2*(2), 262–275. https://doi.org/10.38035/sjam.v2i2.207

[28] Turner, C., & Astin, F. (2021). Grounded theory: What makes a grounded theory study? *European Journal of Cardiovascular Nursing*, *20*(3), 285–289. https://doi.org/10.1093/eurjcn/zvaa034

[29] Makri, C., & Neely, A. (2021). Grounded theory: A guide for exploratory studies in management research. *International Journal of Qualitative Methods*, *20*, 1–14. https://doi.org/10.1177/16094069211013654

[30] Bryda, G., & Costa, A. P. (2023). Qualitative research in digital era: Innovations, methodologies and collaborations. *Social Sciences*, *12*(10), 570. https://doi.org/10.3390/socsci12100570

[31] Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, *9*(1), 3–26. https://doi.org/10.1037/qup0000196

[32] Mortelmans, D. (2025). Thematic coding. In *Doing qualitative data analysis with NVivo* ( (57–87). Springer. https://doi.org/10.1007/978-3-031-66014-6_8

[33] Wang, Z., Zhang, H., Long, X., Wan, S., & Deng, H. (2024). Application of IoT audio technology based on sensor networks in English speaking teaching system. *Measurement: Sensors*, *33*, *101155*. https://doi.org/10.1016/j.measen.2024.101155

[34] Gupta, A., & Nisar, A. (2025). A novel AI-driven graph-swarm THz slice optimizer for terahertz frequency management and network slicing in 6G/7G ORAN networks. *International Journal of Communication Systems*, *38*(7), e70077. https://doi.org/10.1002/dac.7007734

**How to Cite:** Silva-Atencio, G. (2026). Open-RAN: Emerging Trends and Impact on the Telecom Sector in the Digital Age. *FinTech and Sustainable Innovation*. https://doi.org/10.47852/bonviewFSI62026039