Zero Trust Architecture for Secure O-RAN

O-RAN ALLIANCE
WG11 for Security
V1.0

White Paper, May 2024

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany

Register of Associations, Bonn VR 11238, VAT ID DE321720189

Executive Overview

Although 5G is the most secure generation of mobile technology specified to date, the O-RAN ALLIANCE (O-RAN) and various government agencies acknowledge that adoption of open architectures and cloud deployments can expand the attack surface [1]. As sophisticated threat actors have evolved in the Information and Communications Technology (ICT) industrial sector, of which 5G networks are a part, there is increased risk of internal attacks due to advanced persistent threats and lateral movement. Perimeter security alone is no longer sufficient. It is important that 5G and next-G networks providing critical infrastructure and mission critical use cases are built with a zero trust architecture (ZTA) to protect against external and internal threats.

ZTA is the evolution of the zero trust concept to a concrete plan based upon multi-layered security controls that provide confidentiality, integrity, availability, authentication, and authorization protections from internal and external threats. In a ZTA, assets and resources are secured as micro-perimeters and no internal subject, whether human user or digital system, is assumed to be trusted for access to applications and data. ZTA is an important goal for securing critical infrastructure, including 5G Core networks and RAN, to protect against threat actors attempting to gain internal presence in the network for reconnaissance, network disruption, or data exfiltration.

The O-RAN ALLIANCE is committed to pursue a ZTA to achieve a strong security posture to protect against evolving threats. O-RAN ALLIANCE's Work Group 11 (WG11) for Security has evolved O-RAN security requirements with consideration of a ZTA across its thirteen security work items. The specified security requirements and controls provide confidentiality, integrity, availability, authentication, and authorization protections from external and internal threats for O-RAN architectural elements, interfaces, and data. WG11 will continue its pursuit of a ZTA by making incremental improvements consistent with NIST ZTA [2] and CISA Zero Trust Maturity Model (ZTMM) [3], applying all seven tenets of zero trust to O-RAN assets and operational security.

Mobile network operators (MNOs) are adopting ZTA to protect their networks from increasingly sophisticated attacks initiated by internal and external threat actors. To mature the ZTA controls in their networks, MNOs rely on both their security systems and security controls in vendor provided O-RAN architectural elements. The O-RAN ALLIANCE is specifying security controls based on ZTA that consider integration with existing security systems in MNO networks. Standardization alone is not enough to achieve a ZTA, as operational aspects may be specific to the operator's deployment.

O-RAN architectural elements can further enhance the security posture by providing security features that fulfill a ZTA. Service Management and Orchestration (SMO), RAN Intelligent Controllers (RICs), rApps, and xApps can leverage visibility with artificial intelligence (AI) to provide dynamic policy for RAN security and other use cases.

O-RAN's evolving security requirements can be coupled with the security capabilities of O-RAN architectural elements to offer the strongest RAN security posture achieved to date. O-RAN ALLIANCE's currently specified requirements and controls align with the "Initial" stage of the CISA ZTMM and continues to progress towards "Advanced". This paper introduces ZTA and ZTMM with references to guidance documents relevant to the mobile industry and provides an overview of O-RAN's security posture with its goal to incrementally achieve a ZTA.

Table of contents

Introduction

As Open RAN architectures continue to evolve, its specifications, product design, software development, implementation, and operations must continue to be secured with the pursuit of a ZTA. O-RAN ALLIANCE WG11 has made significant progress to incrementally improve the O-RAN security posture and is continuing the ZTA journey with contributions from operators, vendors, government agencies, and academic institutions from around the globe. It is important that the security specifications of 5G and future (6G) generations of mobile systems continue to progress through the ZTA maturity stages with network functions and interfaces secured to protect against external and internal threats. This paper introduces ZTA and ZTMM, with references to guidance documents relevant to the mobile industry from US Government agencies, including National Institute of Standards and Technology (NIST), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA). This paper then describes O-RAN's security posture with its goal to incrementally achieve a ZTA.

Guidance for a ZTA

The following documents provide ZTA guidance relevant to the mobile industry and O-RAN:

- NSA and CISA's Enduring Security Framework (ESF) Open Radio Access Network Security Considerations [1]
- NIST SP 800-207, Zero Trust Architecture (ZTA) [2]
- CISA Zero Trust Maturity Model (ZTMM) [3]
- NSA and CISA's ESF Security Guidance for 5G Cloud Infrastructures [4]

Each of these is described further in the sections below. In addition to these guidance documents, there are other references for specific use cases, such as the US Department of Defense (DoD) Zero Trust Strategy [5] and NSA Maturity Guidance for Zero Trust [6]. The maturity models used by DoD and NSA are similar to CISA's ZTMM with the cross-cutting functions of the CISA ZTMM – Visibility and Analytics, Automation and Orchestration – considered as Pillars instead of cross-cutting functions.

NIST ZTA

NIST SP 800-207 introduces and defines the term "Zero Trust Architecture (ZTA)" as defined by the NIST seven tenets of zero trust [2]:

T1. All data sources and computing services are considered resources

T2. All communication is secured regardless of network location

T3. Access to individual enterprise [operator] resources is granted on a per-session basis

T4. Access to resources is determined by dynamic policy

T5. The enterprise [operator] monitors and measures the integrity and security posture of all owned and associated assets

T6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed

T7. The enterprise [operator] collects information about the current state of assets, network infrastructure and communications and uses it to improve its security posture

It is worth noting Tenets 4, 5, and 7 cover dynamic policy, continuous monitoring, and data collection, respectively, which are often considered to be operational aspects to achieve a ZTA.

CISA ZTMM

CISA acknowledges it is a journey to achieve a ZTA and states "the path to zero trust is an incremental process that may take years to implement". CISA ZTMM [3] establishes a phased approach to incrementally strive towards a ZTA, as modelled in Figure 1. The CISA ZTMM identifies 5 pillars for zero trust: Identity, Devices, Networks, Applications & Workloads, and Data. Each of the pillars has its unique Pillar-specific Functions, and share Cross-cutting Functions that can evolve through four maturity stages to incrementally achieve a ZTA by advancing from Traditional to Initial, then Advanced, and finally to the goal of Optimal. The three cross-cutting functions, Visibility and Analytics, Automation and Orchestration, and Governance, apply to all five pillars. CISA ZTMM enables ZTA critical controls for O-RAN to be implemented in an incremental approach by mapping security controls to the functions across the four ZTMM stages.

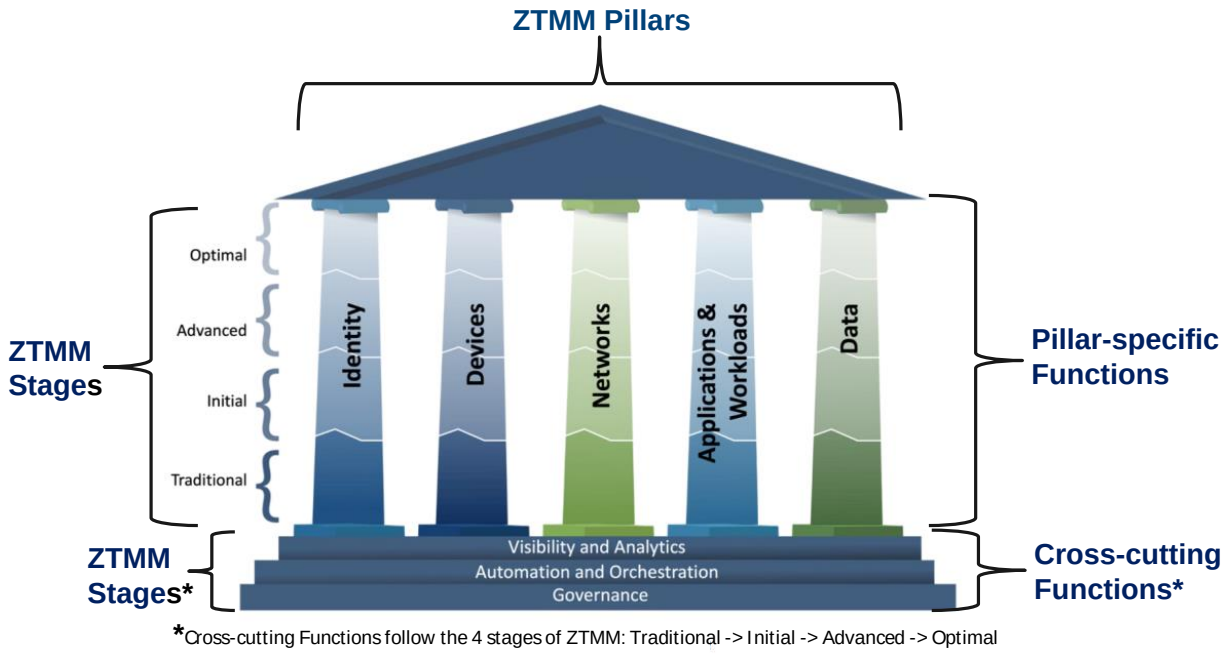

Figure 1. US DHS CISA Zero Trust Maturity Model [3]

ESF

As 5G critical infrastructure evolves to the cloud-native technologies and hybrid cloud deployments, it is increasingly necessary to implement a ZTA that provides protection from external and internal threats, with the assumption the adversary is already inside the network. The Enduring Security Framework (ESF) four-volume publication "Security Guidance for 5G Cloud Infrastructures" [4] provides a playbook for ZTA in 5G cloud deployments. The four volume titles provide useful security guidance for securing Open RAN:

- Part 1: Prevent and Detect Lateral Movement
- Part 2: Securely Isolate Network Resources
- Part 3: Protect Data in Transit, In-Use, and at Rest
- Part 4: Ensure Integrity of Cloud Infrastructure

The ESF's "Open Radio Access Network Security Considerations" [1] determined

- "Security considerations always emerge in new open systems aiming for improved cost, performance, and supply chain benefits. Open RAN shares these security considerations too, and, with continuing efforts by the Open RAN ecosystem, they can be overcome."
- "While there are security considerations due to the expanded threat surface of a multi-vendor Open RAN, other security considerations that apply to the ICT industry at large are also applicable to Open RAN."

The O-RAN ALLIANCE commitment to pursue a ZTA for O-RAN follows the ESF's recommendation to "adopt Information and Communications Technology (ICT) best practices to mitigate these concerns".

Deploying and Operating a ZTA for O-RAN

The ZTA guidance described in the previous chapter, when applied to mobile critical infrastructure, can be summarized with the following four characteristics:

- Network functions are resources secured with micro-perimeters to protect against external and internal threats.
- Authentication and authorization, based on the principle of least privilege, are enforced on a per-session-basis for external and internal subjects.
- Confidentiality and Integrity protection is provided for data-in-use, data-at-rest, and data in-transit on external and internal interfaces.
- Continuous monitoring, logging, and alerting is implemented to detect and respond to security events, including internal lateral movement.

Mobile network operators (MNOs) are adopting ZTA to protect their networks from increasingly sophisticated attacks from both internal and external threat actors. To mature the ZTA controls in their networks, MNOs will rely on both their existing security systems and native security controls in vendor provided O-RAN architectural elements. The O-RAN ALLIANCE will continue to specify vendor support for evolving security controls that meet MNO requirements to achieve a ZTA in O-RAN. For example, specified O-RAN security requirements enforce access controls for each session, encrypt data in transit, protect the integrity of data in transit, and generate logs for security events. In addition, O-RAN architectural elements should be capable to integrate with the operator's identity governance and administration, security policy and compliance management, security information and event management (SIEM), and security posture management (SPM), which are outside the scope of O-RAN ALLIANCE specifications. These operational security capabilities are needed to maintain a ZTA in the operational phase of the deployment.

MNOs will take the ZTA journey in stages following a ZTMM, such as the US DHS CISA ZTMMv2. MNOs will develop tailored approaches to ZTA for O-RAN that incorporate ZTA guidance and specifications provided by the O-RAN ALLIANCE, SDOs (such as 3GPP and ETSI), industry alliances (such as GSMA), and US Government agencies (such as NIST, NSA, and CISA).

O-RAN's Security Posture

O-RAN is evolving RAN with cloud-native network functions (CNFs), artificial intelligence/machine learning (AI/ ML), and standard application programming interfaces (APIs). In a ZTA, O-RAN architectural elements are secured as micro-perimeters. Security controls for confidentiality, integrity, availability, and authenticity continue to be specified so that cloud infrastructure, cloud-native architectural elements, interfaces, and data can be protected from evolving external and internal threats by following the principles of ZTA. The security controls specified by the O-RAN ALLIANCE, as summarized in Table 1, align with a ZTA by protecting external and internal interfaces. For reference, the O-RAN architecture is shown in Figure 2.

Table 1. Specified Security Controls for O-RAN Interfaces

Security Principles	Non-Fronthaul Interfaces						Open Fronthaul Interfaces			
	A1	R1	O1	O2	E2	Y1	C-plane	U-plane	S-plane	M-plane
Confidentiality	TLS	TLS	TLS	TLS	IPsec	TLS		PDCP		TLS/SSH
Integrity	TLS	TLS	TLS	TLS	IPsec	TLS		PDCP		TLS/SSH
Authenticity	mTLS	mTLS	mTLS	mTLS	IPsec	mTLS	802.1X	802.1X	802.1X	mTLS/SSH/802.1X
Authorization	OAuth	OAuth	NACM	OAuth		OAuth	802.1X	802.1X	802.1X	NACM/802.1X
Data Origin Authentication	mTLS	mTLS	mTLS	mTLS	IPsec	mTLS		PDCP		TLS/SSH
Replay Prevention	TLS	TLS	TLS	TLS	IPsec	TLS		PDCP		TLS/SSH

NOTE: 3GPP Access Stratum (AS) Control Plane and User Plane messages that are transported via the Open Fronthaul U-Plane (LLS-UP) are confidentiality and integrity protected by Packet Data Convergence Protocol (PDCP). PDCP security controls remain in place when the message traverses the Open Fronthaul U-Plane.

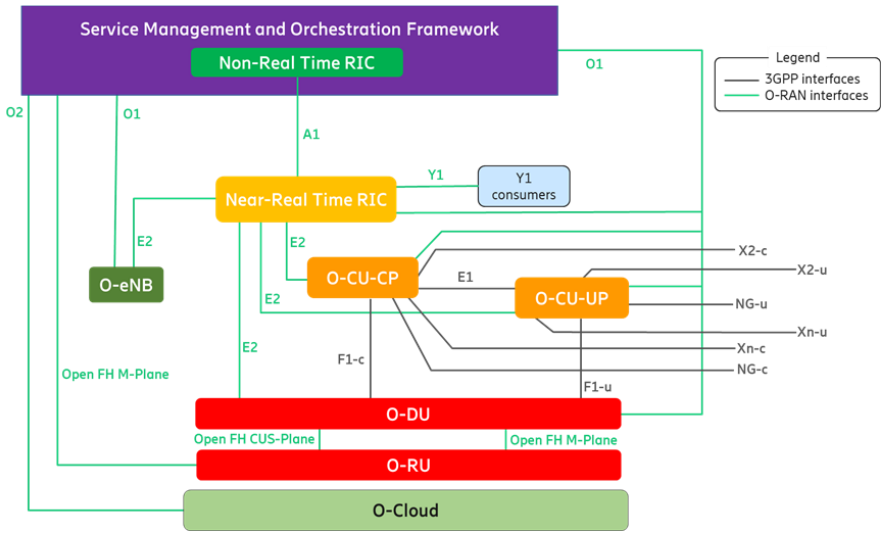

Figure 2. Logical O-RAN architecture diagram [7]

NOTE: O-RAN ALLIANCE specified R1 interface is internal to the Non-RT RIC

In addition to the O-RAN ALLIANCE specified security controls shown in Table 1, security requirements and controls transversal to the O-RAN architecture have been specified, as shown in List 1 below. The specified requirements and controls shown in Table 1 and List 1 align with the "Initial" stage of the CISA ZTMM and are continuing to progress toward "Advanced" stage, followed by "Optimal" stage, as the O-RAN architecture, threats, and controls evolve.

List 1. Examples of Specified O-RAN Security Controls

- Mutual Transport Layer Security (mTLS) and TLS versions 1.2 and 1.3
- Certificate-based mutual authentication using mutual TLS (mTLS) 1.2 and 1.3 with PKI X.509 certificates
- Certificate Management Protocol version 2 (CMPv2) for PKI certificate management across O-RAN
- API security based upon OWASP Top 10 [8]

- Robustness of architectural elements against volumetric DDoS attacks
- Life cycle management for network functions (NFs) and applications
- Signed and protected Software Bill of Materials (SBOM)
- Security event logging
- Secure credentials with encrypted key storage, hardware root of trust, and chain of trust
- Secure O-Cloud with continual run-time scanning, digital signature verification for O-RAN NFs, and hardware acceleration security

O-RAN's security posture is captured in three WG11 security specifications and a technical report that form the pillars of O-RAN security. These four pillar documents, as listed below, can be downloaded from the O-RAN ALLIANCE's public website at O-RAN Specifications [9].

- *O-RAN Security Threat Modeling and Risk Assessment 2.0* [10] – a risk-based threat model and analysis used for building an effective O-RAN security architecture that supports zero trust.
- *O-RAN Security Requirements and Controls Specifications 8.0* [11] – security requirements for each O-RAN interface and component. Requirements address confidentiality, integrity, and availability by defining key controls such as authentication, authorization, replay protection, least privilege access control, and logging.
- *O-RAN Security Protocols Specifications 8.0* [12] – defines implementation requirements for security protocols used by O-RAN including SSH, IPSec, DTLS, TLS 1.2+, OAuth 2.0, SFTP, FTPES, and HTTPS.
- *O-RAN Security Tests Specifications 6.0* [13] – documents the security tests that validate O-RAN implementations of security functions, configurations, and security protocols requirements.

Path to Optimal ZTA in O-RAN

Security work items in WG11 are addressing security across the O-RAN architecture to achieve a ZTA through stages. As stated in the CISA ZTMM, "The path to zero trust is an incremental process that may take years to implement" [3]. CISA ZTMM complements NIST's ZTA by offering a roadmap for organizations to assess their current maturity level and provide guidance on steps to incrementally progress to higher maturity stages. WG11 has an active ZTA work item to conduct a comprehensive study of ZTA for O-RAN and provide recommendations to progress along the ZTMM journey.

WG11 has completed an applicability study of NIST's seven tenets of zero trust and concluded that all seven tenets are applicable to O-RAN. Full realization of tenets 4, 5, and 7 covering the operational aspects of dynamic policy, continuous monitoring, and data collection, respectively, is dependent upon MNO-specific implementations that build upon foundational O-RAN ALLIANCE specifications. Some architectural elements can further enhance the security posture by providing security features that fulfill a ZTA. Service Management and Orchestration (SMO), RAN Intelligent Controllers (RICs), rApps, and xApps can leverage visibility with artificial intelligence (AI) to provide continuous monitoring and dynamic policy, fulfilling tenets 4, 5, and 7.

New O-RAN features, such as O-Cloud, Shared Open-Radio Unit (O-RU), Decoupled SMO, rApps/xApps, and AI/ML will have security built-in to its specifications. WG11 is pursuing a ZTA through a process of threat analysis, risk assessment, and normative security specifications to mitigate risk from the identified threats. When developing a plan for ZTA in O-RAN, it is important to first identify the critical assets to protect from attack, including data, interfaces, architectural elements, infrastructure, and services, as shown in Table 2. The second step is to identify and analyze potential threats to the attack surface, with consideration of external and internal threats. Each WG11 security work item team performs threat modeling and risk assessment with consideration of a ZTA using a risk-based approach. WG11 threat analysis is based upon the Microsoft STRIDE model [14] and risk scoring is calculated from likelihood and impact.

Table 2. O-RAN Assets

Data	Interfaces	Architectural Elements	Infrastructure	Services
• Keys, Credentials • RAN Analytics • UE-Id • UE-Location • AI/ML training data • Configuration data • Logs	• A1, E2, O1, O2, R1, Y1 • Open Fronthaul C-Plane, S-Plane, U-Plane, M-Plane • External Interfaces	• SMO (including Non-RT RIC and rApps) • Near-RT RIC (including xApps) • O-CU-CP • O-CU-UP • O-DU • O-RU • O-eNB • O-Cloud	• O-Cloud HW, OS, and virtualization infrastructure • Hardware and OS of O-RAN PNFs • Fronthaul Gateway, Fronthaul Multiplexer	• AI/ML Services

Note 1: This is not a comprehensive O-RAN asset list. The table provides an overview of the critical assets for security analysis.

nGRG Security

O-RAN ALLIANCE next-Generation Research Group (nGRG) is researching how to secure the platforms on which future mobile networks will be implemented as those networks continue to evolve with more openness and disaggregation. ZTA is guiding the nGRG's definition of security controls that that will be needed to protect the next generation of networks, which could face increasingly sophisticated attacks. An example of potential security controls are attestations across the cloud platform and memory-safe software development techniques. These techniques will help mature O-RAN security, enabling operators to better measure the integrity and security posture of the O-Cloud.

In an upcoming research report on O-RAN platform security to be published in Fall 2024, nGRG will address key techniques expected to play an important role toward achieving security goals in 6G use cases. A nGRG research report for Quantum Security published in December 2023 [15] highlighted the need for quantum-resistant cryptographic algorithms in O-RAN to achieve an Optimal ZTA, as public-key cryptographic algorithms used in mobile networks will become vulnerable to quantum attacks. All published nGRG research reports are available at [16].

Conclusions

Mobile networks are critical infrastructure, which requires a higher security posture based upon a ZTA, as defined by US NIST. Traditional perimeter-based security is insufficient to mitigate internal attacks by insiders and sophisticated threat actors. A ZTA protects against external and internal threats by securing assets as micro-perimeters and protecting internal interfaces with security controls for confidentiality and integrity protection of data-in-transit, at-rest, and in-use, authentication and authorization of external and internal subjects requesting access to resources, and continuous monitoring and logging.

It is important to address all seven tenets of zero trust to achieve a ZTA throughout the network lifecycle. The path to a ZTA can take time and incur costs, so it is advised to take an incremental, risk-based approach to evolve ZTA through ZTMM maturity stages defined by US CISA. This enables vendors and MNOs to embrace ZTA at an acceptable incremental pace to achieve the wanted security posture. To mature the ZTA controls in their networks, MNOs will continue to rely on their existing security systems and security controls natively supported in vendor-provided O-RAN architectural elements. Standardization alone is not enough to achieve a ZTA, as operational aspects may be specific to the operator's deployment.

The O-RAN ALLIANCE is pursuing a ZTA with consideration of external and internal threats in its security analysis. With numerous contributors across industry, government agencies, and academia, O-RAN ALLIANCE WG11 continues to enhance

the O-RAN security posture for each of its assets, including architectural elements, network functions, interfaces, and data. New O-RAN architectural elements and features, such as O-Cloud, Shared O-RU, Decoupled SMO, rApps/xApps, and AI/ML will have security built-in to its specifications. O-RAN ALLIANCE's currently specified security requirements and controls align with the "Initial" stage of the CISA ZTMM. The O-RAN ALLIANCE is well along its ZTA journey to progress towards "Advanced" so that O-RAN suppliers can build-in security and operators can achieve a ZTA in their O-RAN deployments.

References

[1] Open Radio Access Network Security Considerations, Enduring Security Framework (ESF), September 2022.

[2] Zero Trust Architecture (ZTA), NIST SP 800-207, US DoC NIST, September 2020.

[3] Zero Trust Maturity Model (ZTMM), version 2.0, US DHS CISA, April 2023.

[4] Security Guidance for 5G Cloud Infrastructures, Volumes 1 thru 4, Enduring Security Framework (ESF), October-November 2021.

[5] DoD Zero Trust Strategy.

[6] Maturity Guidance for Zero Trust, NSA, March 2024.

[7] O-RAN Architecture Description (OAD), v11.0, O-RAN ALLIANCE, February 2024.

[8] API Security Top 10, OWASP.

[9] https://specifications.o-ran.org/specifications, O-RAN ALLIANCE.

[10] O-RAN Security Threat Modeling and Risk Assessment, Technical Report, v2.0, O-RAN ALLIANCE, February 2024.

[11] O-RAN Security Requirements and Controls Specifications, Technical Specification, v8.0, O-RAN ALLIANCE, February 2024.

[12] O-RAN Security Protocols Specifications, Technical Specification, v8.0, O-RAN ALLIANCE, February 2024.

[13] O-RAN Security Tests Specifications, Technical Specification, v6.0, O-RAN ALLIANCE, February 2024.

[14] STRIDE, Threats - Microsoft Threat Modeling Tool - Azure | Microsoft Learn, Microsoft, August 2022.

[15] Research Report on Quantum Security, O-RAN ALLIANCE, December 2023.

[16] https://www.o-ran.org/research-reports, O-RAN ALLIANCE.

