Review

Distributed Ledgers and Security Mechanisms on Radio Access Networks: A Systematic Review

Daniel Marques * and Dalton Valadares

Posted Date: 28 April 2025

doi: 10.20944/preprints202504.2261.v1

Keywords: radio access networks; RAN; security mechanisms; distributed ledger technology; DLT; internet of things; IoT

 doi:10.20944/preprints202504.2261.v1

Article

Distributed Ledgers and Security Mechanisms on Radio Access Networks: A Systematic Review

Daniel Marques [1,2] **and Dalton Valadares** [1,3]

[1] Federal University of Campina Grande (UFCG)
[2] National Telecommunications Agency (Anatel)
[3] Federal University of Paraíba (UFPB)
* Correspondence: daniel.marques@embedded.ufcg.edu.br

Abstract: 5G is the most recent technology standard for cellular networks, and one of its key elements is the Radio Access Networks (RAN), which furthers the enabling of the 5G basic capabilities: enhanced Mobile Broadband (eMBB), Massive Machine-Type Communication (mMTC), and Ultra-Reliable, Low-Latency Communication (URLLC). To meet the capabilities required by 5G use cases, 5G is distributed, virtualized, and architecturally more complex than previous generations. These capabilities bring benefits but introduce risks and security challenges that must be addressed through controls designed to support and secure 5G services across any operator cloud. Therefore, this paper focuses on studying and evaluating security mechanisms used in RANs. Special attention is given to Distributed Ledger Technologies (DLTs) since they are one of the most studied topics regarding security enhancement. DLTs could bring advantages for improving network security through encryption to protect the information and automate verification and execution of transactions. For this reason, we carried out a systematic review, extracting and analyzing data from 39 papers from 2010 to 2023. Our main results list RAN-related susceptible security dimensions, vulnerabilities, and possible attacks and threats. We also show how DLTs can enhance RANs and present other considered mechanisms to increase RAN security.

Keywords: radio access networks; RAN; security mechanisms; distributed ledger technology; DLT; internet of things; IoT

1. Introduction

This section introduces the motivation for conducting this SLR, states the research questions, presents the main contributions, and defines the scope and limitations of the review.

1.1. Motivation

During the development of the fifth generation of wireless technology, also called 5G, the first steps considered the definition of use cases. This stage identified bottlenecks in previous technologies, especially insufficient spectra, the inability to absorb the predicted growing number of connected devices, and new use cases from emerging QoS requirements, characteristics, and mobile applications [1,2]. So, to address this and other issues, the 5G development focuses on three usage scenarios [3,4]:

- *Enhanced Mobile Broadband (eMBB)* to increase speed and capacity. The expected requirements for this case are a data transmission speed of up to $20Gbps$ and a latency of less than $7ms$.
- *Ultra Reliable, Low-Latency Communications (URLLC)*, which aims to guarantee low latency and high reliability to comply with requirements of vertical market segments such as industrial, health, transportation, and aviation. Their target requirements are a probability of error from 10^{-5} to 10^{-8} and a latency of less than $3ms$.
- *Massive Machine-Type Communications (mMTC)* support a massive number of connected objects, such as Internet of Things (IoT) environments. To reach this use case, it needs a density of up to 1 million devices per square kilometer and a battery life of up to 10 years without recharging.

 doi:10.20944/preprints202504.2261.v1

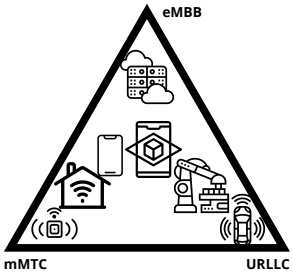

Figure 1. ITU 5G usage scenarios.

These scenarios can lead to improved user experiences, more connected environments, and opportunities for innovation and economic growth [5]. Once different functionalities demand different resources, a specific user can use three scenarios at distinct intensities (Figure 1). However, these innovations come with several challenges. Some of them are:

- the necessity of an increasing amount of antennas due to the use of higher frequencies.
- the demand for ensuring compatibility between 5G and previous networks considering latency requirements.
- the growing number of devices.
- and deployment complexity, to name a few.

Furthermore, the evolution of mobile communication brings about not only hardware problems. The most recent mobile networks are immersed in *softwarization* and *virtualization* [6]. Softwarization is the possibility of running functionalities in software components instead of hardware, which brings high flexibility and reconfigurability to networks. Virtualization is the software/hardware splitting by creating virtual instances of network resources, which permits software to run on commercial off-the-shelf (COTS) hardware. These new paradigms dissociate the insertion of new functionalities and network updates from the necessity of hardware upgrades, which can introduce a reduction in capital (CAPEX) and operational (OPEX) expenditure when updating or introducing new functions and network configurations, especially due to functional splits and Network Slicing [7] (NS). However, softwarization and virtualization insert new vulnerabilities into the network, for example, network development and deployment could be prone to human errors and their complexity can increase the potential for flaws and bugs [8].

In addition to these and other challenges, one more arises: network security. The intrinsic characteristics of 5G bring another plethora of security challenges [9]. The transition from 4G to 5G demands 5G non-standalone (5GNSA) networks, in short, 5G access networks with a 4G core. However, 5GNSA networks are vulnerable, for example, to Denial of Service (DoS) attacks, as they bring 4G vulnerabilities from the beginning. Even 5G standalone (5GSA, the *pure* 5G) networks are susceptible to exploitation once they are based on software-defined networking (SDN) and network function virtualization (NFV), which use the HTTP and REST API protocols, well-known and widely used on the Internet, including by malicious agents [10].

Considering the mentioned scenarios, it is necessary to address new 5G cybersecurity issues due to the rising application of cloud computing, edge computing, and the convergence of mobile and traditional IT networks by creating new vulnerabilities. For example, adversaries can maliciously deploy their own devices and applications to exploit the open nature of the mobile edge. This approach could enable traffic to be sniffed without authorization and reach results close to the Man-in-the-Middle attack.

This topic is relevant to policymakers and public sector regulators as well. For instance, the Brazilian Telecommunications Agency (Anatel) [11] established a governance model through the Working Group for Cybersecurity and Critical Infrastructure Risk Management (Cyber WG), which defines Cybersecurity[1] as “actions aimed at operational security to ensure that information systems

[1] https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1

 doi:10.20944/preprints202504.2261.v1

can withstand events in cyberspace capable of compromising the availability, integrity, confidentiality, and authenticity of data stored, processed or transmitted, and the services that these systems offer or make them accessible".

In this sense, we can mention Distributed Ledger Technologies (DLTs) among the technologies applied to improve security in 5G network components. We observe that the more the 5G technology evolved, considering its requirements and specifications, the more proposals utilize DLTs technology to register different information sources. Among the DLTs, blockchain stands out as a DLT used to register, authenticate, and validate assets, transactions, and interactions. Furthermore, blockchain records data and manages identification in different networks in a trusted, decentralized, and secure manner [12]. Consequently, some studies aim to apply blockchain in radio access networks to leverage 5G networks. One of the main interests of using blockchain in telecommunication networks lies in the Multi-access Edge Computing (MEC) paradigm. Thus, blockchain could supply a decentralized edge computing marketplace matching edge infrastructure vendors with retailers without a single control point [13]. For instance, this approach can help to develop a commercial model to access edge cloud infrastructure. So, we have expanded the scope to investigate possible other DLTs that could enhance RAN security.

Furthermore, we have considered studying how various security mechanisms could enhance RAN security and how these technologies can increase system resilience. In this sense, we speculate DLTs could perform a significant role in RAN security since they function in a trusted, decentralized, and secure manner. We hypothesize that DLTs can improve communication security due to their characteristics. This paper also brings other RAN security approaches discussed in academia to identify which security topics are studied beyond DLTs.

To elaborate this study, we decided to carry out a Systematic Literature Review (SLR) [14,15], which allows us to investigate a specific area by determining and following a systematic process that other researchers can use in the future to validate or update our results and can be applied to study different topics, including those related to this work, such as Distributed Ledger Technologies [16], Access Networks [17], and Cybersecurity [18]. It is important to note that an SLR demands a slow and gradual process to avoid possible issues such as loss of repeatability, impact on stability, risk of bias, and negligence on proper documentation. This established process allows to properly focus on answering the research questions as defined by the SLR protocol.

Therefore, this work presents the results of a systematic review of ways to improve security in RANs to give a structured overview of identified vulnerabilities, threats, attacks, and possible security dimensions applicable to detect and mitigate harmful effects and plan networks less susceptible to different risks and menaces.

1.2. Scope and Limitations

One of the main objectives of this work is to investigate how DLTs are applied to increase security in RANs. Thus, it is important to highlight that DLT is a broader term that refers to any digital ledger maintained across a network of nodes in a decentralized, distributed manner. Some types of ledgers use different mechanisms to achieve agreement among network participants: For example [19–21]:

- *Blockchain* uses a chain of blocks to record and verify transactions. Each block contains a set of transactions validated by a consensus mechanism.
- *Directed Acyclic Graph (DAG)*, a ledger based on a graph structure to record and verify transactions. These transactions are linked in a directed graph rather than a linear chain. DAG ledgers can be more scalable and efficient than linear chains, and they are often used for applications such as IoT and micropayments.
- *Distributed Consensus Ledger*, a distributed ledger that uses a consensus mechanism to validate transactions and achieve agreement among network participants. It does not necessarily use a chain of blocks to record transactions.

 doi:10.20944/preprints202504.2261.v1

- *Federated Ledger*, a distributed ledger controlled by a consortium or group of organizations. In this case, participants have a defined level of access and control over the ledger and consensus is reached among participants rather than through a public blockchain or consensus algorithm.
- *Hybrid Ledger*, that combines different types of DLT.

Considering these definitions, DLTs have a relevant role in this review. However, to establish a comparative reference, the online search considered the term *security mechanisms* to include other approaches applied to RANs.

Furthermore, we can see other security topics discussed in the accepted papers. Vulnerabilities in *Radio Resource Control (RRC)* mentioned in some papers, including access control, outdated assets, and authentication, are discussed as the main vulnerabilities of RRC protocols.

Other accepted papers investigate *Intrusion Detection Systems (IDS)* and *Intrusion Prevention Systems (IPS)*. Denial of Service (DoS) and Man-in-the-Middle (MitM) attacks are the most relevant risks considered in these papers. In this case, the proposed systems are anomaly detection-based systems with different implementations and hybrid systems that merge IDS and IPS with other technologies.

The *Fronthaul (FH) interface* that provides connectivity between the radio and the baseband units in the RAN is an attention point in the accepted papers. Suggested ways to deal with the clear-text nature of the FH data include the insertion of security standards and protocols.

Security in the *Network Slicing*, a feature that creates virtual slices across the RAN to allow unique network access for several enterprises and applications, is also a recurrent topic. The proposals to improve slicing security include a certificateless signature scheme and a virtual private network.

It is important to note that the accepted papers come from the search string developed during the preparation of the SLR protocol; that is, this review focuses on the works brought by the search carried out in the repositories of scientific articles defined in the structuring of the protocol.

1.3. Research Questions

This review studies application security mechanisms that increase privacy and security in RANs by managing access and authentication for entities in these networks. It also evaluates other security mechanisms in the same context Thus, we define the following research questions.

- What are the main threats to the Radio Access Networks (RANs)?
- How are Distributed Ledger Technologies (DLT) applicable to enhancing RANs?
- What do studies apply to increase security in RANs?
- How do studies apply DLTs to increase security in RANs?
- What are the advantages and disadvantages of DLT usage to improve security in RANs?
- What are the proposed future works (open challenges)?

1.4. Contributions

This work aims to identify mechanisms to improve RAN security and how they do it. Thus, following the established systematic literature review protocol, we have considered 39 papers published in journals and conferences after the search and selection phases. Our first result is general information regarding the quantitative analyses of the extracted data. Then, we present vulnerabilities, threats, affected security dimensions, and proposed solutions. We could verify trends in the use of DLTs on the RANs and specific security concerns related to the Fronthaul (FH), Network Slicing (NS), and Radio Resource Control (RRC). Furthermore, the remaining contributions of this article are:

- We elaborated the SLR protocol, which can be used to replicate or update this study in the future.
- We defined and reviewed 39 papers considering they explore threats, vulnerabilities, attacks, and solutions for RAN security.
- We analyzed and presented the information extracted from the accepted papers, classifying threats, vulnerabilities, and solutions.

 doi:10.20944/preprints202504.2261.v1

- We presented the state-of-the-art related to security issues in RAN scenarios, discussing important points.

1.5. Review Structure

The remainder of this work is organized as follows. Section 2 briefly introduces some security concepts, Radio Access Networks, and Distributed Ledger Technologies. Section 3 describes the threat model adopted for this work. Section 4 explores the threats, vulnerabilities, and solutions discussed in the accepted papers. We interprets the findings of the papers, discussing the main implications of the results and comparing the identified security solutions, in Section 5. We conclude this study in Section 6. Additionally, Appendix A presents the systematic literature review protocol and Appendix B shows the general results from the collected data, considering quantitative information.

2. Background

This section presents the theoretical basis of this systematic review. It includes security elements, the Radio Access Network framing, and Distributed Ledger Technologies.

2.1. Security Concepts

It is important to define some key security concepts to lay a foundation and contribute insights for this research, helping to classify the accepted papers. This way, based on the Internet Engineering Task Force (IETF) RFC 4949, Internet Security Glossary, Version 2 [22], we can specify:

- *Attack*: a malicious attempt to collect, disrupt, deny, degrade, or destroy the system information or the system itself.
  - Attack Surface [23], in the context of the Radio Access Network (RAN), is the set of potential entry points that adversaries can exploit to gain unauthorized access to the network. For example, we can cite the introduction of Network Slicing (NS), a feature that creates virtual slices across the RAN to allow unique network access for several enterprises and applications [24]. However, malware from a slice may be leveraged to infect another slice in the same hardware. A certificateless signature could be a countermeasure, as discussed in Subsection 5.2.5.
- *Security*: established and maintained measures to protect the system/component/data. It may involve six functions:
  - Deterrence, the threat discouraging.
  - Avoidance, reducing the probability of a loss or the value of the potential loss.
  - Prevention, countermeasures to minimize possible security violations.
  - Detection, identifying occurred or in progress violations.
  - Recovery, actions to restore the normal state of a system.
  - Correction, updating the security architecture to reduce or eliminate risks.
- *Threat*: an intentional or accidental danger that might occur if an attacker is successful. The considered threats [25] in this paper are:
  - Destruction of information or other resources.
  - Corruption or modification of information.
  - Theft, removal, or loss of information or other resources.
  - Disclosure of information.
  - Interruption of services.
- *Vulnerability*: a security breach, that could be a flaw or weakness in a system's design, implementation, or operation and management, and could be exploited to violate a system.

As important as the definition of these previous terms is the circumscription of security dimensions [26,27], which are sets of security measures designed to address a particular aspect of network security.

 doi:10.20944/preprints202504.2261.v1

According to the references, there are eight sets focused on the protection against the majority of the threats:

- *Access control*, the protection against unauthorized use of network resources.
- *Authentication*, the confirmation of entity identities.
- *Availability*, the ensuring of authorized access and information availability.
- *Communication security*, the protection against data diversion or interception.
- *Data confidentiality*, the protection against data unauthorized disclosure.
- *Data integrity*, the guarantee of correctness or accuracy of the data.
- *Non-repudiation*, the correctness in the association between actions and actors.
- *Privacy*, the protection of the information.

It is possible to verify that this approach is more comprehensive than the CIA security triad[2], a famous guiding model in information security, which only includes confidentiality, integrity, and availability among its components.

2.2. RAN Architecture

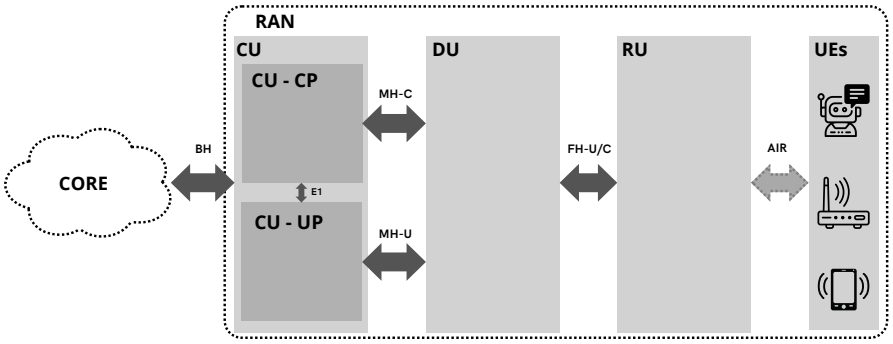

Figure 2. RAN primary architecture.

Although this work does not focus on a specific generation, we explain the 5G RAN architecture as a reference in this subsection since this SLR selected 4G, 5G, and generation-agnostic papers. The primary 5G RAN architecture is designed in 3GPP Rel-15 specifications [28] (Figure 2).

The RAN [29,30] is the central part of the wireless communication system as it is responsible for connecting the user equipment (UE) to the core network (CN) and includes a set of base stations and user equipment devices, such as smartphones, routers, or IoT devices [31]. Nonetheless, a typical RAN involves two essential units, the radio unit (RU) and the baseband unit (BBU):

- The *Radio Unit (RU)* contains radio functions and is located near the antennas.
- The *Baseband Unit (BBU)* is responsible for radio management, resource utilization, sharing, and other operations like modulation and demodulation, bit-to-symbol mapping, and coding and decoding.

Early cellular systems [32] used integrated BBUs and RUs components. However, this architecture suffered from radio frequency signal propagation loss in the electrical cable feed [33] since some of the signal energy dissipates in the cable and the components [34]. So, the concept of distributed RANs (D-RANs) arose to address this issue by separating the BBU and RU components and connecting them through a common public radio interface (CPRI).

The next step in the RAN evolution was the introduction of Cloud Radio Access Networks (C-RANs), in which some cellular network functions are relocated to the cloud infrastructure. This operation involves migrating the BBU to the cloud while keeping the RU at the base station. The BBU is connected to the RU through a high-speed and low-latency Fronthaul communication channel, activated by the enhanced common public radio interface (eCPRI). This open and Ethernet-based interface

[2] https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/

 doi:10.20944/preprints202504.2261.v1

has ubiquitous applications and enables different types of traffic [35]. C-RANs offer advantages such as reduced capital and operational expenditures, improved energy efficiency, and dynamic resource allocation.

This evolution paved the virtualization of the RAN functions and their use on generic hardware platforms [36]. Virtualized Radio Access Networks (vRANs) enable telecommunication carriers to perform their base-band functions as software running on not necessarily proprietary hardware.

2.2.1. Protocol Layer Stack

Another relevant step in the RAN evolution is the segregation of the BBU into Centralized Unit (CU) and Distributed Unit (DU). In 5G networks, the 3GPP Release 15 defined this split, which is especially relevant to Open RAN [37]:

- The *Centralized Unit (CU)* implements the higher layers of the 3GPP stack, namely the Radio Resource Control (RRC) layer, the Service Data Adaptation Protocol (SDAP) layer, and the Packet Data Convergence Protocol (PDCP) layer, among others. It is divided into two interfaced modules, one dedicated to the user plane (UP) and the other to the control plane (CP), due to the *Control and User Plane Separation (CUPS)* architecture. The CUPS architecture provides flexibility for network improvement compared to the conventional architecture where both planes have a less pronounced separation [38].
- The *Distributed Unit (DU)* is responsible for some functionalities of the physical layer, the Medium Access Control (MAC), and Radio Link Control (RLC), among others.

The distribution of mobile network services among various protocol layers is essential for efficient and effective communication within the network. This distribution allows for function separation, enabling better management, optimization, and scalability. Each network layer can focus on specific functions, making it easier to understand, maintain, and upgrade the system due to the network service division. Layered architecture also provides interactions between adjacent layers through defined interfaces that simplify the network. Furthermore, network layering brings interoperability, efficient resource allocation, scalability, flexibility, ease of troubleshooting, and generation integration. The generation integration is a relevant service since it allows, for example, handover between different base stations. However, cross-generation handover is not always a smooth transition. For instance, the core network-based integration between 4G and 3G has slow mechanisms that enable hard handovers and access selection [39], a concern that can be addressed by protocol layering.

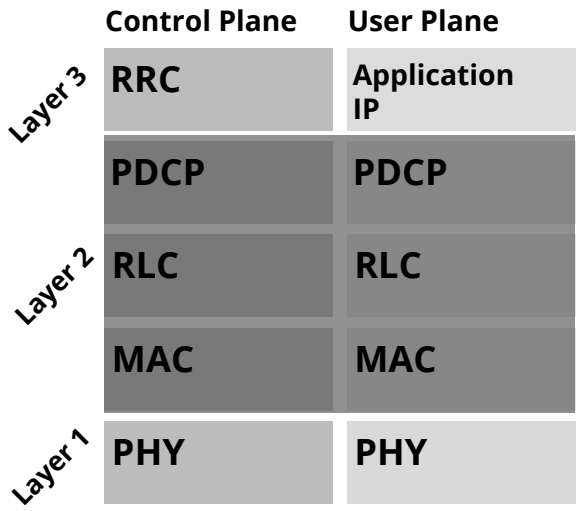

Figure 3. RAN protocol stack.

The RAN protocol stack is divided into three layers [40] (Figure 3). The first one is the *Physical (PHY)* layer and, in 4G-LTE networks, is based on orthogonal frequency-division multiplexing (OFDM)

 doi:10.20944/preprints202504.2261.v1

transmission. It maps logical channels and provides transport channels to the above MAC layer. The 5G-NR PHY layer brings various enhancements to meet IMT-2020 requirements, such as eMBB, URLLC, and mMTC support; scalable numerology to face different deployment scenarios, bandwidth sizes, and carrier frequencies; massive multiple-input multiple-output; dynamic time division duplexing; power efficiency; and waveforms beyond OFDM [41].

The second layer, or the *Data Link* one, is responsible for data bearing, among other functions. It includes:

- The *Medium Access Control (MAC)* protocol multiplexes RLC packet-data units (PDUs) through logical channels and performs mapping between logical and transport channels [42]. Other MAC layer functions include uplink and downlink scheduling, scheduling information reporting, hybrid-ARQ processing and retransmissions in 4G-LTE (automatic repeat request, ARQ, is an error-control method based on acknowledgments), and multiplexing/demultiplexing data for carrier aggregation. [41].
- The *Radio Link Control (RLC)* protocol's main functions include segmentation and concatenation, retransmission handling, duplicate detection, and in-sequence delivery to upper layers [42]. Regardless of its generation, the RLC layer supports three transmission modes – Transparent Mode (TM) to broadcast data, Unacknowledged Mode (UM) to support data loss-tolerant services such as voice, and Acknowledged Mode (AM) with an ARQ retransmission mechanism for services such as TCP/IP and RRC signaling that require data reliability. RLC UM and AM modes support data segmentation and resegmentation at the transmitter, and AM provides duplicate detection [41].
- The *Packet Data Convergence Protocol (PDCP)* provides data packet encryption and integrity protection for the control plane and, for the user plane, ciphering/deciphering, header compression/decompression using Robust Header Compression (RoHC) for IP traffic, in-sequence delivery, duplicate detection, and retransmission (continuously in 5G-NR networks, especially during handovers in 4G-LTE ones) [39,41]. The PDCP layer does not have synchronicity constraints with the lower layers, and 3GPP assumes that the 4G dual connectivity functions can be used as a baseline in 4G/5G interworking since PDCP functions are access/service-agnostic [42].

The *Network* layer is the third one and has specificities for each plane. The user-plane third layer includes the *Service Data Adaptation Protocol (SDAP)*, a 5G-NR innovation, which does not exist in 4G-LTE and previous mobile communication generations. Its essential role is to map traffic from quality of service (QoS) flows[3] to suitable data radio bearers [43].

The control-plane third layer manages wireless resource allocation assignments, such as signaling, and implements the lower part of the protocol stack. It includes the RRC protocol [44,45], which stands out most for this review, as shown in Subsection 5.2. The RRC is a protocol responsible for connecting the base station and UEs. In addition to managing resource allocation, the RRC protocol tunnels the Non-Access Stratum (NAS), an upper-layer protocol stratum between the core network and UEs, to support the mobility and session management procedures. Up to the 4G-LTE, RRC manages active connections to carry user traffic and idle connections to provide global reachability for UEs. 5G-NR networks introduce a new state named RRC inactive, enabled if there is no activity from UE for a short time. This way, the session is suspended by moving to the RRC inactive state to reduce system access, save power, and optimize mobility [46,47]. It is important to note that, unlike the other protocols mentioned, the RRC is only in the control plane.

The 5G RAN architecture flexibility allows computing hardware pools to handle the higher layer processing of user and control planes. The Baseband Unit (BBU) split between the Centralized Unit (CU) and the Distributed Unit (DU) brings adaptability to the network and permits different protocol implementations. To cite a few, there are the Heterogeneous Cloud Radio Access Networks (HC-RANs)

[3] QoS flow is a stream between the UE and the data network that follows the data flow with different levels of priority, data rate, latency, and so on.

 doi:10.20944/preprints202504.2261.v1

[48], in which architecture combines C-RAN and heterogeneous networks (HetNets) to take advantage of small cells transmitting signals with low power within a traditional macro cell network, and Fog Computing Radio Access Networks (F-RANs) [49], which exploit the edge and storage capabilities of fog computing to address Fronthaul constraints of C-RANs and HC-RANs. Furthermore, open RAN deployments stand on vRAN. However, it is implemented based on disaggregated components, connection through open and standardized interfaces, and interoperability across different vendors.

2.3. Distributed Ledger Technologies

Distributed Ledger Technologies (DLTs) is a comprehensive definition of multi-party networks that aim to reach an agreement over a set of shared data and its validity by consensus. These networks function in a decentralized/distributed manner and do not necessarily have a central operator or authority, although they may not be in a trusted environment [50–52]. One example is blockchain technology, a DLT consisting of a chain of data and transaction blocks used by Bitcoin cryptocurrency.

DLTs have three layers: *protocol*, *network*, and *data*. Each layer has one or more components involved in the DLT system creation or operation. A *component* is a set of related processes for the system's functioning. A series of actions to achieve a specific goal or goals involved in the operation of a component is called a *process*. The protocol layer has rules for system operation. The network layer interconnects processes that implement the protocol. The data layer flows the information.

In this work, the network layer is the most relevant since it determines the right of entry to the DLT network. A gatekeeper can restrict access to specific entities in a closed system, since this may have more static membership than open systems. However, access to an open network can be unrestricted and, therefore, there is more dynamicity in membership access granting. There are also semi-open networks, in which prospective participants have their access candidacy evaluated by existing network members.

The greater the network openness, the more likely it is to present vulnerabilities, especially to Sybil attacks, in which the adversary aims to create numerous fake identities to gain influence over the network. The identity of a user or an entity is external-source information, so the DLT network cannot confirm the identity authenticity by itself and, therefore, deal with Sybil attacks alone. To face this issue, open systems usually have a *Sybil attack-resistance mechanism*. For instance, proof-of-work (PoW) [53], a block proposer method in which the nodes solve puzzles to reach an agreement, was the exclusive Sybil attack-resistance mechanism adopted by early open DLT systems. It is hard to fake register transactions in a PoW-assisted DLT since this mechanism aims to attach a cost to participating in the block producer selection algorithm. PoW, however, increases this additional cost to honest entities, too.

This way, another Sybil attack-resistance mechanism raises to address this extra cost by staking endogenous resources (e.g., native assets) to choose the next transaction register: proof-of-stake (PoS) [53], a mechanism that randomly selects validators for block creation based on the amount that tokens holders stake. PoW-based systems have increased register difficulty, but it is easy to verify. PoS-based systems are less resource-intensive but can be vulnerable to other attacks, such as nothing-at-stake attacks that can record parallel subchains in a blockchain and grinding attacks that can manipulate the stake selection procedure.

The Sybil attack-resistance mechanism helps to achieve network entity unanimity about the system validation. The validation process occurs through:

- the *transaction validation*, to verify the individual transaction compliance with the established rules;
- the *record validation*, to verify the record can be done according to the protocol; and
- the *transaction finality*, to determine if the transaction is finalized and, therefore, immutable.

For this reason, PoW, PoS, and other similar mechanisms are also called *Sybil attack-resistance and finality mechanisms*. A public DLT needs a way to reach consensus beyond a Sybil attack-resistance and finality mechanism [50]. In the literature, numerous cases cite PoW and PoS as consensus mechanisms

 doi:10.20944/preprints202504.2261.v1

[54–60]. However, a consensus mechanism is a tool to perform frequently secure updates on the distributed ledger, maintaining important properties such as fault tolerance, resilience, and delay perseverance [61]. It aims to guarantee that all network participants agree to register for events. This way, it ensures that all nodes have the same ledger copy. For instance, in the Bitcoin blockchain, the Nakamoto consensus is a simple mechanism that chooses the blocks that form a valid chain with greater difficulty [51]. Closed DLT networks, in turn, have more participant verification. Due to that, they usually take advantage of consensus mechanisms such as:

- *Paxos* [62] provides a fault-tolerant implementation in an asynchronous message-passing system in which clients send commands to a leader that assigns these commands and, in a second step, a message is sent to a set of acceptor processes.
- *Raft* [60] elects a leader to coordinate the replication actions of the DLT.
- *Practical Byzantine Fault Tolerance (PBFT)* [60] is also based on a leader-follower approach but demands agreement among a high percentage of the participants to attach a new transaction.

It is important to note that, even under the protection of Sybil attack-resistance and finality mechanisms, open DLT networks are prone to other different attacks [50]. For instance, if adversaries have the majority of the votes of a system, they can replace records from honest nodes. It is known as a 51% attack in PoW-based DLTs [63] and a similar attack in PoS-based DLTs [64] is called a long-range attack. These attacks rely on the ability to generate the longest chain.

3. Threat Modeling

The 5G RAN architecture flexibility, especially the BBU split between the CU and the DU, brings adaptability to the network and permits different protocol implementations, as explained in Subsection 2.2. Nonetheless, these characteristics could further new vulnerabilities [65]. So, based on this architecture, it is possible to define the attack surfaces. The attack surfaces include the RAN elements and the interfaces in between, and they are:

- *User Equipment* **(UE)** is the equipment served by the RAN, which can be a smartphone, a sensor, or anything that can connect to the RAN.
- *Air Interface* **(Air)** is the interface between the UE and the RAN.
- *Radio Unit* **(RU)** contains radio functions and is located near the antennas.
- *Fronthaul* **(FH)** is the interface between the RU and the DU.
- *Distributed Unit* **(DU)**, where the most decentralized base band functionalities are deployed.
- *Midhaul* **(MH)** is the interface between the DU and the CU.
- *Centralized Unit* **(CU)**, where the high-layered base-band functionalities are deployed.
- *Backhaul* **(BH)** is the interface between the RAN and the Core Network.

Another attack surface considered is *Network Slicing* **(NS)** [66], which is related to the physical network resources division between different logical networks. Each sliced logical network can be applied to a specific scenario and serve different tenants.

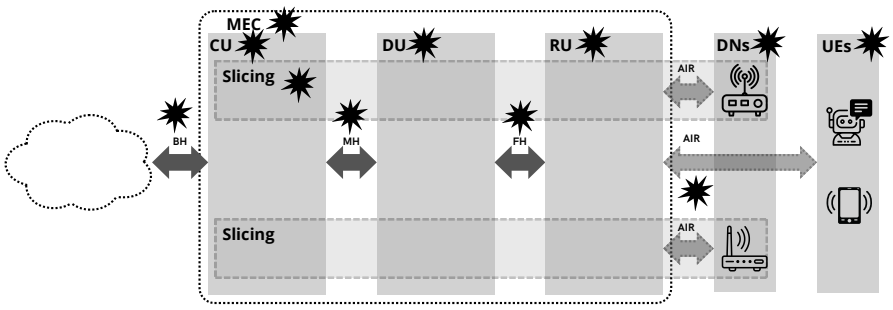

Figure 4. Defined attack surfaces.

Figure 4 shows the attack surfaces and possible expansions. Our threat model includes the previous attack surfaces, which can be expanded when mobile networks connect or provide services

 doi:10.20944/preprints202504.2261.v1

and resources to *decentralized networks* **(DN)** since recent access networks, especially 5G RAN, are heavily virtualized [67]. RAN virtualization allows the connection of the mobile networks through some DNs, which, in this case, may share the same threats and vulnerabilities that affect Radio Access Networks since the virtualization of the networks makes the RAN boundaries less precise. Some DNs that could expand the attack surface when connected to or provided by a Radio Access Network are Mobile ad-hoc networks (MANET) [68], Peer-to-Peer (P2P) networks [69], Device-to-Device (D2D) networks [70], and Machine-to-Machine (M2M) networks [71], to cite a few.

Virtualized RANs can benefit from *Multi-Access Edge Computing* **(MEC)** [72], the decentralized computing concept that can use computing resources of the Radio Access Network and permits users to access the closest servers, taking advantage of low latency, for example. When MEC is associated with access networks, which occurs more frequently in 5G networks, the MEC servers also expand the attack surface.

4. Vulnerabilities, Threats, Attacks, and Solutions

In this section, we present the review's technical findings. These include an overview of the security threats, attacks, and vulnerabilities identified in Radio Access Networks and a description of the existing security solutions and countermeasures. We aim to analyze the research trends and identify possible gaps in the current body of knowledge.

4.1. Overview of Security Threats and Vulnerabilities in Access Networks

We start this subsection by listing all the accepted papers, in Table 1, according to their main subjects: Blockchain (**BC**), Fronthaul (**FH**), Intrusion Detection System (**IDS**) / Intrusion Prevention System (**IPS**), Radio Resource Control (**RRC**), and Network Slicing (**NS**). The remaining papers are arranged as *Others* since they cannot be classified into these previous themes and study various topics.

Then, we list the main vulnerabilities of each paper in Table 2. These vulnerabilities are arranged according to the following four classes [109]:

- *Process*: when the vulnerability is related to common processes.
  - Authentication issues, such as lack of, weak, or broken authentication. If RAN nodes are not properly authenticated, attackers could impersonate legitimate devices, carry out brute-force attacks, or decrypt communications.
  - Broken access control or lack of its validation. In this case, adversaries can access sensitive network functions and exploit misconfigured interfaces to inject malicious traffic or disrupt services.
  - Data storage problems, i.e., unprotected storage. This may result in leakage of private data and network settings.
- *Code*: when the vulnerability is related to the software and development process. In this sense, it is important to highlight the difference between coding and development. While development focuses on managing actions and overseeing the software creation process, coding is focused on implementation, translating ideas into actionable code using programming languages [110]. Since analyzing these details is beyond the scope of this work, it was decided to consider them under the same heading for the sake of simplicity. In this context, we can cite encryption mechanisms that are both conceptual (designed through development) and practical (implemented via coding) and, so, can then be viewed at different implementation layers.
  - Lack of cryptography, which attackers can exploit to lack private data or set up a rogue BTS.
  - Codification or development problems, such as the absence of secure coding practices. Vulnerabilities in the software running on the network or in the UE can arise from poor coding practices, such as buffer overflows, injection flaws, improper error handling, lack of input validation, which could allow attackers to inject malicious commands or data.
  - Cryptographic algorithm lag or weakness. Weak or deprecated cryptographic algorithms can make RANs susceptible to attacks, i.e., brute-force attacks.

 doi:10.20944/preprints202504.2261.v1

Table 1. Subjects of the papers.

Subject	Paper	Reference
BC	BC-RAN: Cloud radio access network enabled by blockchain for 5G	[73]
	Blockchain-enabled wireless communications: a new paradigm towards 6G	[74]
	Distributed Network Slicing Management Using Blockchains in E-Health Environments	[75]
	Design of a Security and Trust Framework for 5G Multi-domain Scenarios	[76]
	Data Broker: Dynamic Multi-Hop Routing Protocol in Blockchain Radio Access Network	[77]
	Future Industry Internet of Things with Zero-trust Security	[78]
	Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications	[79]
	Blockchain-based fog radio access networks: Architecture, key technologies, and challenges	[80]
	Evaluation of soft computing in intrusion detection for secure social Internet of Things based on collaborative edge computing	[81]
	Resource Sharing and Trading of Blockchain Radio Access Networks: Architecture and Prototype Design	[82]
	Radio optical network security analysis with routing in quantum computing for 5G wireless communication using blockchain machine learning model	[83]
	Hedera: A Permissionless and Scalable Hybrid Blockchain Consensus Algorithm in Multi-Access Edge Computing for IoT	[84]
FH	Securing Ethernet-based optical fronthaul for 5G network	[85]
	Secure Open Fronthaul Interface for 5G Networks	[86]
	Transport Security Considerations for the Open-RAN Fronthaul	[87]
	Open-RAN Fronthaul Transport Security Architecture and Implementation	[35]
IDS/IPS	Detecting DoS and DDoS Attacks by Using CuSum Algorithm in 5G Networks	[88]
	Attacks and failures prediction framework for a collaborative 5G mobile network	[89]
	The Novel System of Attacks Detection in 5G	[90]
	An edge based hybrid intrusion detection framework for mobile edge computing	[91]
	A highly secured IDS for IoT using EXPSO-STFA feature selection for LAANN to detect attacks	[92]
RRC	Authentication Protocol for an IoT-Enabled LTE Network	[93]
	On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks	[94]
	LTE Security Disabled: Misconfiguration in Commercial Networks	[95]
	5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol	[46]
	AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks	[31]
	UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework	[96]
	Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G	[97]
NS	A Fast Authentication Scheme for Cross-Network-Slicing Based on Multiple Operators in 5G Environments	[98]
	Advanced 5G Network Slicing Isolation Using Enhanced VPN+ for Healthcare Verticals	[99]
Others	Security Analysis of a Femtocell Device	[100]
	Insecurity of Operational Cellular IoT Service: New Vulnerabilities, Attacks, and Countermeasures	[101]
	Adversarial Trends in Mobile Communication Systems: From Attack Patterns to Potential Defenses Strategies	[102]
	Link-based penalized trust management scheme for preemptive measures to secure the edge-based Internet of Things networks	[103]
	Intelligent privacy preservation proctol in wireless MANET for IoT applications using hybrid crow search-harris hawks optimization	[104]
	Cyber-Security Measures for Protecting EPES Systems in the 5G Area	[105]
	Uncovering Insecure Designs of Cellular Emergency Services (911)	[106]
	Privacy-aware access control (PAAC)-based biometric authentication protocol (Bap) for mobile edge computing environment	[107]
	Unveiling the Insecurity of Operational Cellular Emergency Services (911): Vulnerabilities, Attacks, and Countermeasures	[108]

- *Communication*: when the vulnerability is related to protocols or data transmission. This class of vulnerability may affect RANs due to loss of confidentiality if an attacker exposes sensitive user and network data, loss of integrity if adversaries modify communications or inject malicious data, loss of availability due to jamming attacks or physical tampering, and reputation damage, that can reduce user trust and lead to regulatory penalties.
  - Lack or weakness of security mechanisms, such as resistance to tampering.
  - Communication problems can include unreliable communication channels, ease of UE impersonation, and susceptibility to eavesdropping due to the openness of the wireless interface.
- *Operation*: when the vulnerability is related to the nodes' use or configuration.
  - Outdated assets can include lack of updates, network exposure, incorrect software configuration, and bad user practices, to name a few.

The reference paper [109] presents a *Device* category. However, it is not used in this work since it does not apply to Radio Access Network environments.

Although there may be more than one vulnerability in each accepted paper, and each vulnerability could be categorized into more than one class, we consider one main vulnerability per article and allocate it into a single class. However, we also list other vulnerabilities we identified in the accepted papers beyond the main vulnerability, and inserted them in the *Other works* column of Table 2.

 doi:10.20944/preprints202504.2261.v1

Table 2. Main vulnerabilities.

Vulnerability Class	Vulnerability	Main papers	Other works
Code	Codification/development	[102]	[94]
	Cryptographic algorithms	[104] [79]	[92] [78]
	Lack of cryptography	[106] [108]	[101] [99] [77] [105] [78] [79] [100] [84] [85] [86] [104] [107] [95]
Communication	Communication problems	[103]	[97] [80] [105] [73] [91] [46] [106] [108] [74] [76] [79] [96] [83] [102] [94] [90] [35]
	Lack or weakness of security mechanisms	[85] [88] [90] [86] [87] [105] [35] [101]	[93] [99] [77] [81] [80] [103] [82] [92] [89] [91] [31] [76] [96] [100] [102]
Operation	Outdated assets	[75] [76] [94] [95]	[100] [93]
Process	Access control	[100] [46] [89] [91] [92] [31] [80] [81] [82] [83]	[97] [101] [105] [95] [78] [74] [76] [90] [85] [86] [107] [103]
	Authentication	[93] [98] [99] [78] [107] [96] [97] [84]	[105] [46] [95] [31] [106] [108] [79] [100] [102] [90] [87] [35] [104] [103]
	Data storage	[73] [74] [77]	[97] [101] [105] [82] [89] [91] [46] [95] [31] [76] [79] [96] [102] [90] [93] [35] [107] [103]
Main papers:	Papers whose main vulnerability is as described		
Other works:	Papers that study such vulnerability in addition to its main one		

Table 3 presents the identified threats and the corresponding security dimensions that these threats can affect, as defined in subsection 2.1.

Table 3. Main threats.

Security dimension	Main threat	Main papers	Other works
Access control	Corruption or Modification of Information	[92] [80] [81]	[31] [100]
	Destruction of Information or Other Resources	[100] [89] [91] [83]	—
	Disclosure of Information	[31]	[91] [46] [79] [107]
	Theft/Removal/Loss of Information or Other Resources	[46] [82]	—
Authentication	Disclosure of Information	[98] [78] [97]	[93]
	Theft/Removal/Loss of Information or Other Resources	[93] [84]	—
Availability	Interruption of Services	[106] [108] [99] [96]	—
Communication security	Disclosure of Information	[101]	[85] [86] [87] [35]
	Theft/Removal/Loss of Information or Other Resources	[85] [86] [87] [35]	[101]
Data integrity	Corruption or Modification of Information	[73] [74] [77]	—
	Destruction of Information or Other Resources	[104] [75]	—
Non-repudiation	Corruption or Modification of Information	[76]	[105] [95] [90] [103]
	Disclosure of Information	—	[105] [76] [102] [90] [103]
	Interruption of Services	[102] [103] [88] [90] [105] [94]	[76]
	Theft/Removal/Loss of Information or Other Resources	[95]	[102]
Privacy	Disclosure of Information	[79] [107]	—
Main papers:	Papers whose main threat is as described		
Other works:	Papers that study such threat in addition to its main one		

Figure 5 shows the relationship between the threats identified in the articles and the security dimensions [27], with the horizontal axis representing the security dimensions and the vertical axis representing the threats. We can see that not all dimensions are related to all threats, which conforms with the ITU-T Recommendation X.805 [27]. This Recommendation, discussed in Section 2.1, considers that *Non-repudiation* security dimension needs to be considered to face all the defined threats. However, in the accepted papers, *Non-repudiation* security dimension was especially remembered to face *Interruption of Service* threats. On the other hand, other dimensions were applied to face a wider range of threats. *Access control* security dimension is an example since it was considered to deal with four different threats.

 doi:10.20944/preprints202504.2261.v1

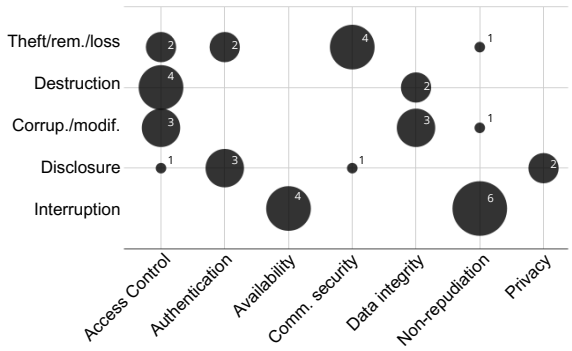

Figure 5. Threats and security dimensions.

We then classify these papers by their main threats and vulnerabilities, as seen in Table 4. This Table shows, for example, that Fronthaul issues are related to *Communication* vulnerabilities and threats associated with *Theft, Removal, or Loss of Information or Other Resources*, and blockchain is a recurrent subject to treat *Process* vulnerabilities and *Corruption or Modification of Information* threats.

Table 4. Subjects vs. threats and vulnerability classes.

	Threat					
Vulnerability	**Interruption**	**Disclosure**	**Corrup./modif.**	**Destruction**	**Theft/rem./loss**	***Total***
Communication	IDS/IPS: 2 Others: 2	Others: 1			Fronthaul: 4	9
Process	RRC: 1 Slicing: 1	Blockchain: 1 RRC: 2 Slicing: 1 Others: 1	Blockchain: 5 IDS/IPS: 1	Blockchain: 1 IDS/IPS: 2 Others: 1	Blockchain: 2 RRC: 2	21
Code	Others: 3	Blockchain: 1		Others: 1		5
Operation	RRC: 1		Blockchain: 1	Blockchain: 1	RRC: 1	4
Total	10	7	7	6	9	39

Interruption: Interruption of Services
Disclosure: Disclosure of Information
Corrup./modif.: Corruption or Modification of Information
Destruction: Destruction of Information or Other Resources
Theft/rem./loss: Theft, Removal, or Loss of Information or Other Resources

In this research, we could identify the different attack surfaces considered in each accepted paper. Table 5 summarizes these findings, in which we can note that the most considered surface is the User Equipment (UE). Other recurrent surfaces considered are the Centralized Unit (CU), Decentralized Networks (DN), and Multi-access Edge Computing (MEC). We found an average of 1.7 considered attack surfaces per article.

4.2. Considered Attacks

Various attacks can menace Radio Access Networks. Table 6 shows 29 attacks we identified in the accepted papers, summarizes these attacks, and lists the documents in which we find them. Due to their similarities, DoS and DDoS attacks are analyzed together, as are Flooding and Signaling attacks.

We can see in Table 6 that the most recurrent attacks cited are DoS/DDoS, MitM, false data injection, eavesdropping, identity theft, and flooding/signaling. The identified attacks have various purposes and intrusion methodologies. To simplify RAN attack analysis and help future works, we propose a novel RAN attack classification into five categories:

- *Network unavailability (NU)* attacks make it impossible for the user to access the network.
- *Data corruption (DC)* attacks aim to intercept, inject, corrupt, delete, or steal data to manipulate communication.
- *Unauthorized access (UA)* attacks include malicious actions to gain unauthorized access.

 doi:10.20944/preprints202504.2261.v1

Table 5. Summary of considered attack surfaces.

Paper	UE	Air	RU	FH	DU	MH	CU	BH	NS	DN	MEC	Paper	UE	Air	RU	FH	DU	MH	CU	BH	NS	DN	MEC
[100]	X							X				[99]		X							X		
[93]	X									X		[78]										X	
[94]	X	X					X					[103]											X
[95]	X											[104]										X	
[85]				X								[92]										X	
[46]	X						X					[79]	X		X		X		X				
[88]	X										X	[105]	X	X									
[73]	X									X		[31]	X	X									
[89]									X			[106]	X										
[98]									X			[80]										X	
[74]	X		X		X		X					[107]											X
[90]	X	X										[108]	X										
[75]									X			[35]				X							
[86]				X								[81]	X									X	X
[91]											X	[96]	X						X				
[101]	X											[97]	X	X					X				
[76]		X						X			X	[82]										X	
[87]				X								[83]				X		X		X			
[102]	X	X										[84]	X									X	X
[77]										X		**Total**	20	8	2	5	2	1	6	3	4	10	7

Table 6. Considered attacks.

Attack class	Attack	Papers	# papers
Network unavailability (NU)	**DoS/DDoS**	[87] [31] [105] [106] [108] [35] [79] [81] [91] [92] [89] [99] [102] [103] [88] [90] [107] [75] [78] [83] [46] [85] [94]	23
	Flooding/signaling	[80] [76] [92] [99] [102] [46] [94]	7
Data corruption (DC)	**MitM**	[87] [86] [96] [31] [101] [35] [79] [82] [74] [104] [88] [90] [98] [46] [85] [93]	16
	False data injection	[87] [86] [105] [35] [74] [81] [89] [102] [88] [107] [100] [46] [93]	13
	Replay	[87] [105] [35] [79] [98] [93]	6
	Insider	[73] [91]	2
	Spamming	[101]	1
Unauthorized access (UA)	**Backdoor**	[81] [91] [92] [90] [107] [85]	6
	Hijacking	[106] [84] [81] [89] [88] [94]	6
	Sybil	[79] [77] [84] [76] [104] [83]	6
	Tampering	[105] [73] [80] [82] [74] [103]	6
	Malware spreading	[105] [91] [103] [88]	4
	User-to-root	[91] [103]	2
Data leakage (DL)	**Eavesdropping**	[87] [86] [97] [35] [82] [74] [76] [102] [46] [85]	10
	Impersonation/spoofing	[87] [35] [76] [95] [100] [93] [31] [104] [102] [103]	10
	Identity theft	[31] [76] [92] [102] [107] [78] [100] [93]	8
	Sniffing	[86] [73] [91] [103] [90] [85]	6
	Cryptanalytic	[79] [81] [104]	3
	Quantum	[86] [85]	2
	Phishing	[88]	1
	Wormhole	[83]	1
Physical resource spoliation (PR)	**Jamming**	[31] [105] [102] [103] [83]	5
	Rogue BTS	[96] [31] [97] [94]	4
	Bidding-down	[97] [90]	2
	Physical damage	[83] [100]	2
	Signal overshadowing	[96] [31]	2
	Resource exhaustion	[89]	1

- *Data leakage (DL)* attacks aim to acquire and steal confidential and sensitive information.
- *Physical resource spoliation (PR)* attacks are the ones that menace hardware and other physical resources.

This attack categorization will be detailed in future work.

Furthermore, concerning the vulnerability [109], threat, and security dimension [27] classifications discussed in this review, we identified which vulnerabilities these attacks exploit and which threats they pose to RANs. In addition, we could verify which security dimensions need to be applied to face these attacks.

ITU-T Recommendation X.805 security dimensions were defined to address different aspects of network security. In addition, it provides a mapping of security dimensions to the security threats. This mapping shows that not all security dimensions are applicable to address all possible threats. For example, the *privacy* security dimension protects information that may derive from the observation of the network activity and it is indicated to protect communications against disclosure of information threats only. However, the *non-repudiation* security dimension is designated to address all ITU-T

 doi:10.20944/preprints202504.2261.v1

Recommendation X.805 threats. Consequently, we can identify the *non-repudiation* security dimension to face all defined attack classes. One possible inference from this finding is that implementing tools to prevent *an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions* [27] is a good starting point to deploy RAN security measures.

Beyond the *non-repudiation* security dimension, *access control* was identified as relevant to avoid network unavailability, unauthorized access, data leakage, and physical resource spoliation attacks. As defined in ITU-T Recommendation X.805, the access control security dimension ensures *that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services, and applications*. In this way, user and entity identification is important to enhance RAN security in a broader definition, as well-established access control politics can help prevent agents with hidden interests from penetrating the network.

Related papers show that strategies based on the *communication security* security dimension can face data corruption attacks by ensuring that *the information is not diverted or intercepted as it flows between authorized end points* [27]. In addition, *availability* security dimension helps address issues related to network unavailability attacks since this security dimension *ensures that there is no denial of authorized access to network elements, stored information, information flows, services, and applications due to events impacting the network*.

Table 7. Main vulnerabilities, threats, and relevant security dimensions related to defined attack classes.

Class	Vulnerabilities	Threats	Security dimensions
NU	Access control Lack/weakness	Disclosure Interruption	Non-repudiation Access control Availability
DC	Access control Lack/weakness Authentication Data storage	Disclosure Interruption	Non-repudiation Comm. security
UA	Access control Lack/weakness Comm. problems Data storage	Disclosure Interruption Corrup./modif.	Non-repudiation Access control
DL	Access control Data storage	Disclosure Interruption	Non-repudiation Access control
PR	Access control Data storage Authentication Lack/weakness	Disclosure Interruption	Non-repudiation Access control
Lack/weakness:	Lack or weakness of security mechanisms		

Our findings exposed in Table 7 detail Table 6 and show that regardless of the attack class, adversaries take advantage mainly of *access control*, *data storage*, and *lack or weakness of security mechanism* vulnerabilities. In addition, the main threats identified in the accepted papers (Table 3) are *disclosure of information* and *interruption of services*. Based on these data, we can infer that adversaries may have two main purposes when attacking access networks: intercepting private information and disrupting communications.

Data breach costs are increasing continuously. The average global cost of a data breach in 2024 increased by 10% from the previous year, reaching *US*$4.88 million [111]. This is the highest total ever. Network outages can cause major troubles. Cloud platform issues [112] disrupted networks and harmed various businesses and institutions worldwide, from healthy services to airline and train companies. These examples show that academic concerns identified in this review are connected with current issues. Furthermore, recognizing possible aggression targets can help optimize resources to increase Radio Access Network security.

 doi:10.20944/preprints202504.2261.v1

Papers in which blockchain is the main subject consider unauthorized access and physical resource spoliation attacks as the focus menaces. Fronthaul-subjected papers consider data corruption and physical resource spoliation attacks as the main fronthaul menaces. Papers considering IDS and IPS as focal topics bring greater concerns about network unavailability, unauthorized access, and physical resource spoliation attacks. RRC-focused papers understand data leakage and physical resource spoliation attacks are the main RAN menaces. Papers studying slicing security consider physical resource spoliation attacks the main RAN security concerns. These findings are detailed in Table 8, which shows the attack classes from Table 7 and the subjects and the number of papers per subject from Table 1.

Table 8. Subjects vs. attack classes.

Subject	*Attack classes*					*Total of papers*
	NU	**DC**	**UA**	**DL**	**PR**	
Blockchain	7	5	10	8	10	12
Fronthaul	3	4	1	3	4	4
IDS/IPS	5	4	5	4	5	5
RRC	3	5	1	6	6	8
Slicing	1	1	0	0	2	2
Others	6	5	5	4	6	8

It is interesting to note that, according to Table 8, the most comprehensive attack class is physical resource spoliation. Regardless of the subject, we can infer that the open-air interface is an important aggression door against radio access networks due to its physical openness. Nonetheless, network slicing papers bring concerns about physical resource spoliation since radio resource allocation is one of its main features [98,99].

Beyond physical resource spoliation attacks, the remaining subjects assign attention to different attack classes. Blockchain works pay attention to unauthorized access attacks since the decentralization of network functions and their influence on the QoS are some of the main motivations to adopt blockchain in RANs [113,114].

Fronthaul-related papers [35,85–87] focus on data corruption attacks. This concern comes from the clear-text nature of the Control, User, Synchronization, and Management (CUSM) planes and their direct encapsulation over Ethernet, which could expose the FH to different menaces.

Papers that study IDS and IPS focus on anomaly detection systems, which can evaluate traffic overwhelm by, for example, monitoring resources. This way, it is understandable that these papers target their efforts to study ways to understate the effects of network unavailability and unauthorized access attacks [81,88].

RRC and data leakage are related topics in some papers as well. It is important to note that the RRC protocol is responsible for connection establishment, maintenance, handover, reselection, and release. This way, an attacker with some control over the RRC protocol can access all kinds of data [31,46,93–97].

4.3. Description of Suggested Security Solutions

Table 9 lists the proposed solutions for each paper, sorting them by class and purpose [109]. We can verify that there are 12 DLT-based proposed solutions among the 39 accepted papers, but the only DLT considered is Blockchain. The considered solution classes are:

- Approach/Mechanism.
- Architecture.
- Framework.
- Methodology/Method.
- Model/Algorithm.
- Protocol.
- Scheme.

 doi:10.20944/preprints202504.2261.v1

The purposes of the different solutions listed in the accepted papers are:

- Detect.
- Detect/Mitigate.
- Mitigate.
- Planning.

Table 9. Proposed Solutions.

Solution class	Purpose	Proposed solution	Paper (Year)
Approach/Mechanism	Detect/Mitigate	Prevention mechanism against bidding-down attacks	[97] (2023)
		Suite of solution approaches	[101] (2021)
	Mitigate	Isolation of healthcare vertical slicing approach	[99] (2022)
		Blockchain-ledger safeguard mechanism	[77] (2021)
		Blockchain to secure the NS management layer in private networks	[75] (2021)
Architecture	Detect	Blockchain network IDS architecture	[81] (2023)
	Detect/Mitigate	Blockchain-based Fog-RAN	[80] (2022)
		Cyber-security measures applied to a power plant to detect/mitigate unwanted actions	[105] (2022)
	Mitigate	Blockchain-unified architecture for resource sharing and trading	[82] (2023)
		Blockchain-enabled architecture	[73] (2020)
Framework	Detect	Intrusion detection framework for IoT	[92] (2022)
		Several security prediction agents framework	[89] (2021)
		Intrusion detection framework for MEC	[91] (2021)
		Framework for verification of the control-plane	[46] (2019)
		Security testing framework	[95] (2019)
	Detect/Mitigate	Security testing framework	[31] (2022)
		Suite of standard-compliant solutions	[106] (2022)
		Suite of standard-compliant solutions	[108] (2023)
	Mitigate	Blockchain zero-trust framework for IoT	[78] (2022)
		Trustworthy and secure Blockchain paradigm for 6G networking	[74] (2021)
		Blockchain security and trust framework	[76] (2021)
		Privacy preserving Blockchain framework	[79] (2022)
	Planning	Security testing framework	[96] (2023)
Methodology/Method	Detect	Security analysis methodology	[100] (2011)
		Blockchain method for analysing radio optical networks	[83] (2023)
		Adversarial trends analysis methodology	[102] (2021)
	Detect/Mitigate	Security analysis methodology	[94] (2018)
Model/Algorithm	Detect	Attack detection algorithm	[90] (2021)
	Detect/Mitigate	Security algorithm to detect and mitigate DoS/DDoS attacks	[88] (2020)
	Mitigate	Permissionless, scalable Blockchain consensus algorithm	[84] (2023)
Protocol	Mitigate	Authentication protocol for the IoT-enabled LTE network	[93] (2016)
		WireGuard security protocol	[85] (2019)
		MACSec security protocol	[86] (2021)
		MACSec security protocol	[87] (2021)
		MACSec security protocol	[35] (2023)
		IoT security protocol in MANET	[104] (2022)
		Authentication protocol for MEC	[107] (2023)
Scheme	Detect/Mitigate	Trust-based routing scheme	[103] (2022)
	Mitigate	Authentication scheme for slicing	[98] (2021)

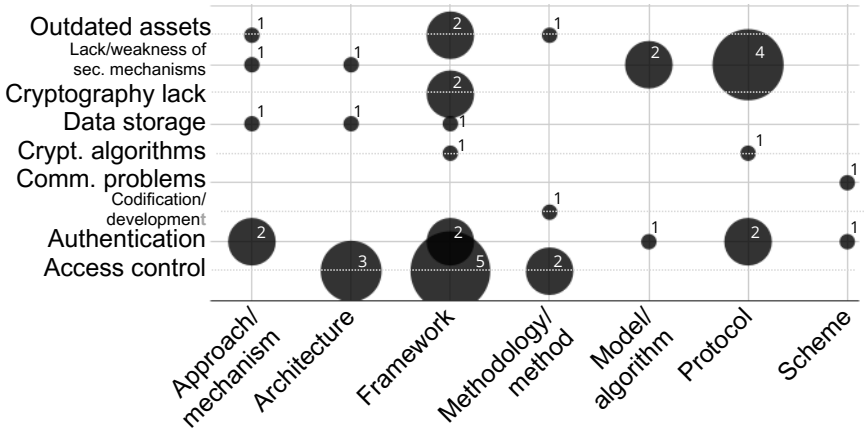

Figure 6. Vulnerabilities and solution classes.

Most solutions are related to the *Framework* class and target their efforts to mitigate threats. Figure 6, which is generated from Tables 2 and 9, shows the relationship between the vulnerabilities and the applied solution classes to oppose them. The horizontal axis represents the solution classes, and the

 doi:10.20944/preprints202504.2261.v1

vertical axis represents the vulnerabilities. Although the solution classes are diffusely applied to the vulnerabilities studied, we can see that the *Framework* class was widely used in different vulnerabilities, especially to reinforce security in *Access Control*. Likewise, the *Protocol* class was more applied for the vulnerability *Lack or Weakness of Security Mechanisms*.

The discussions in the accepted papers emphasize various threat mitigation strategies to enhance security in RANs and related systems. These strategies include addressing security threats in edge-based IoT networks, developing defense systems against threats in 5G networks, improving security in multi-access edge computing networks, and detecting and preventing attacks such as DoS, Botnet, Network intrusion, and MitM attacks.

While vulnerability detection is also discussed in the accepted papers, generally the focus is on implementing measures to mitigate threats and strengthen the security posture of RANs. Threat mitigation strategies such as real-time detection of core IDS and development of AI/ML-based algorithms for intrusion detection in 5G and future 6G networks [90], and evaluation of trust values of devices in cloud-based networks [103] are highlighted as possible approaches to enhance security.

Therefore, it can be inferred that the collection of papers presents more threat mitigation strategies than vulnerability detection measures among their proposed solutions. This can be confirmed by checking Tables 9 and 10. The collected data shows that 18 papers focused on mitigating threats, 10 embraced vulnerability detection and threat mitigation, 10 were orientated to detect vulnerabilities, and one was concerned with planning RAN security.

Table 10. Solution purpose vs. threats and vulnerability classes.

	Threat					
Vulnerability	**Interruption**	**Disclosure**	**Corrup./modif.**	**Destruction**	**Theft/rem./loss**	***Total***
Communication	D/M: 3 Detect: 1	D/M: 1			Mitigate: 4	9
Process	Mitigate: 1 Planning: 1	D/M: 2 Mitigate: 3	Detect: 2 D/M: 1 Mitigate: 3	Detect: 4	Detect: 1 Mitigate: 3	21
Code	Detect: 1 D/M: 2	Mitigate: 1		Mitigate: 1		5
Operation	D/M: 1		Mitigate: 1	Mitigate: 1	Detect: 1	4
Total	10	7	7	6	9	39
D/M:	Detect/Mitigate					

The accepted papers discuss various threat mitigation strategies to enhance RAN security. Some of the key threat mitigation approaches mentioned in the document include:

- Implementing security principles during state transitions and mobility to protect sensitive personal data and ensure network confidentiality [35,79,99].
- Mitigating threats and addressing vulnerabilities in edge-based IoT networks such as authentication issues, network attacks, and user-to-root attacks to safeguard data [103].
- Developing defense systems against threats in 5G networks, including malware, phishing, hacking, DoS, DDoS, SQL injections, and MitM attacks [88].
- Detecting and preventing attacks such as DoS, Botnet attacks, Network intrusion, MitM attacks, and Quantum attacks to mitigate risks related to theft or loss of information and resource threats [86].

These mitigation strategies aim to strengthen the security posture of RANs and related networks by addressing potential threats and vulnerabilities. Furthermore, these papers provide insights into vulnerability detection strategies to verify and address potential weaknesses in RANs. Some important points regarding vulnerability detection discussed in these papers include the evaluation of trust values of devices in cloud-based networks to prevent security attacks and study other security threats beyond DoS attacks and detection of security threats in edge-based IoT networks to prevent network security compromising [103]; detection and prevention of DDoS attacks by the proposed network topology for enhanced attack detection [88]; and development of AI/ML-based algorithms for intrusion detection in 5G and 6G networks to provide cybersecurity measures and protect users [90].

 doi:10.20944/preprints202504.2261.v1

These discussions highlight the importance of proactive vulnerability detection measures to strengthen the security infrastructure of RANs and ensure the resiliency of network communications. Nonetheless, it is important to underline that detection and mitigation are crucial for a comprehensive RAN security strategy. Detection and mitigation measures are essential for catching and addressing these issues before they can be exploited. New threats and attack vectors emerge constantly, so detection and mitigation are relevant tools to deal with them.

We could verify attackers take advantage mainly of *access control*, *data storage*, and *lack or weakness of security mechanism* vulnerabilities (Table 2), and, the main threats identified in the accepted papers (Table 3) are *disclosure of information* and *interruption of services*, regardless of the attack class. Although security in access networks requires a broader approach, given the variety of possible attacks, it may be a relevant initiative to develop and implement security tools in RANs considering these vulnerabilities and threats mentioned. Furthermore, according to ITU-T Recommendation X.805, the non-repudiation security dimension is useful to face all defined attack classes, and we could corroborate this by analyzing the accepted articles. So, ensuring the authorship of acts and actions and recording them for future reference can help deploy security tools in access networks.

Unfortunately, we did not identify many papers focusing on planning RAN security from the ground up. We have identified only one work on security planning [96]. This proactivity can offer a holistic approach to security issues in a RAN environment [115]. Proactive security measures built into the design phase can prevent vulnerabilities from arising in the first place, possibly making it difficult to carry out attacks. Minimizing the RAN attack surface is possible since we consider security during the RAN planning stage. Automated processes for security tasks and pre-configured responses to potential threats can optimize personnel activities. Furthermore, a secure foundation sets the stage for future RAN expansion or technology incorporation, reducing the risk of vulnerabilities being introduced later. This way, efficient RAN planning involves architectural flexibility, security measures, and smart resource management.

It is possible to approach RAN security planning with the *Security by Design* concept [116], which emphasizes integrating security measures into the design and architecture of systems from the outset. It can be useful by reducing the risk of vulnerabilities, ensuring a more robust network, addressing security requirements holistically, and allowing for risk assessment and mitigation strategies. Secure design principles can enhance the network's resilience against attacks and can implement standard compliance. Another relevant point is that considering security throughout the lifecycle can ensure ongoing protection against evolving threats. Finally, other approaches that can enrich RAN security include Zero Trust Architecture [117] and Decryption of Network Traffic [118], which we can leave for future work.

5. Discussion

In this section, we summarize the answers to research questions, aim to interpret the paper's findings, discuss the key implications of the results, and compare the different identified security solutions. We also target to address the challenges in future research.

5.1. Answers to Research Questions

5.1.1. RAN Threats

Focusing now on the research questions to list the approaches present in the accepted papers, we begin by identifying threats to the security of access networks. These RAN issues underscore the importance of implementing comprehensive security measures to mitigate risks and safeguard the integrity, confidentiality, and availability of Radio Access Networks. So, we verified the most cited possible RAN attacks and referred these cited attacks to various RAN threats considering the ITU-R X.805 [27] threat classification.

MitM, where an attacker can impersonate some RAN node, inject false packets, intercept legitimate packets, introduce delays, and perform passive wiretapping [31,35,74,79,82,85–88,90,93,96,98,101,104].

 doi:10.20944/preprints202504.2261.v1

These attacks can lead to network disruption and interruption of services [31,35,74,79,85,87,88]. Considering the ITU-R X.805 threat classification, MitM attacks are more related to *Theft, Removal, or Loss of Information or Other Resources*, *Disclosure of Information*, and *Interruption of Service* threats, as we have discussed in previous sections.

Attackers can inject fake control messages or replay intercepted legitimate control messages to disrupt some RAN component operation and affect network functionality [87]. According to the ITU-R X.805 threat classification, we can relate it to *Theft, Removal, or Loss of Information or Other Resources* threat.

DoS, DDoS, and flooding attacks on communication between the core network and RAN, as well as the radio frontend, pose threats to RAN security by overwhelming network resources and disrupting services [31,35,46,74,78,79,85,87–89,91,92,102,103,105,106,108]. We can infer these attacks are correlated to the ITU-R X.805 *Interruption of Service* threat.

Active eavesdropping on the 2G radio interface is possible due to the lack of mutual authentication between users and the network. So, it motivates bidding-down attacks, which aims to force the connection to a less secure standard [35,76,82,85–87,102]. In this case, *Disclosure of Information* and *Interruption of Service* are the main ITU-R X.805 threats.

Vulnerabilities in protocols such as Signaling System 7 (SS7) [101,102] in 3G networks and GPRS Tunnelling Protocol (GTP) [102] in 3G and 4G networks can be exploited for eavesdropping, financial theft, data interception, and privacy leaks, closer to the ITU-R X.805 *Disclosure of Information* threat.

These cited RAN issues underscore the importance of implementing comprehensive security measures to mitigate risks and safeguard the *Access Control*, *Authentication*, *Non-repudiation*, *Data Confidentiality*, *Communication Security*, *Data Integrity*, *Availability*, and *Privacy*, all the security dimensions of Radio Access Networks.

5.1.2. DLT Usage to Enhance RANs

The accepted papers show that DLTs can enhance access networks in various ways. Some of the key applications of DLTs in RAN security and functionality are:

- DLT-based intrusion detection can be employed to detect and prevent intrusions. Furthermore, it can ensure trusted communications [81].
- The use of consensus algorithms in the RAN environment could help to ensure the integrity and security of transactions and communications by preventing malicious insider threats [73–75,79–81,84].
- A decentralized monitoring framework can build trust between nodes and track distributed transactions to guarantee integrity and security [74,76,77,79–81,83].
- Decentralized networks can enhance RAN performance, and the use of consensus mechanisms and job offload functions can reduce the computational burden [74,76–82].
- Furthermore, DLTs can facilitate traceability of transactions [73], collect user-level application information to develop distributed learning models [80], and improve resource planning by using smart contracts [79].

So, DLTs, particularly blockchain technology, can be leveraged to enhance trust, data sharing, and network performance in Radio Access Networks, offering innovative solutions to address various security and operational challenges in RAN environments. Nonetheless, resource allocation stands the most among possible DLT applications on RANs, as we can see in Subsection 5.2.1.

5.1.3. Approaches to Increase RAN Security

The most comprehensive topic covered in this review is increasing security in access networks. So, several approaches are suggested in the accepted papers to enhance RAN security. Mentioned key strategies include:

 doi:10.20944/preprints202504.2261.v1

- Use of security protocols, such as MACSec, to provide authentication, integrity, confidentiality, and replay protection, to the Fronthaul. However, it may face challenges in meeting security standards [35,86,87].
- The adoption of secure communication frameworks to support SDN controllers and provide reliable and flexible network management to resist internal and external attacks [75,80,103].
- Establishing edge super data centers comprising BBUs and edge servers with technologies like blockchain, artificial intelligence, and big data to ensure safety, facilitate secure access control, tracking, and supervision of mobile equipment [74,79].

These approaches aim to strengthen RAN security by incorporating trust mechanisms, secure communication frameworks, ledger safeguard mechanisms, and advanced contract mechanisms. Furthermore, integrating technologies can enhance overall network security and resilience.

5.1.4. DLTs to Increase RAN Security

Focusing on the use of DLTs, it is possible to note that they permit various ways to improve security in access networks. The accepted papers show some DLT uses to enhance RAN security, and examples of RAN security enhancement due to DLT use are:

- RANs can reach secure and transparent resource allocation and transactions due to the ability of DLTs to increase resource trading since they enforce participants to behave honestly and follow predefined rules [82].
- DLTs may lead to increased measures such as encryption to protect assets, prevent cheating, and safeguard legitimate interests [75,76,78,82,83].
- Some papers argue that integrating DLTs into RANs can result in better load balance, service latency, and resource utilization if, for example, subnetworks are used to enhance processing rates and throughput performance [74,77,78,80,83,84].
- Distributed ledgers can provide scalability and flexibility while ensuring security by combining permissioned and permissionless elements [74,76,77,79,83,84].
- RANs can reach the safety and integrity of transaction data by using a DLT-based decentralized environment to monitor network resources and trust between nodes [74,76,77,79–81,83].
- The combined use of DLTs and Zero-Trust framework may provide stronger secure authentication and deliver a software-defined security perimeter, for example, in IoT systems [76,78].

These examples demonstrate that DLTs, especially blockchain technology, can improve security in Radio Access Networks in various contexts ways.

5.1.5. Advantages and Disadvantages of DLT Usage to Improve Security in RANs

Cited advantages of using DLTs to improve RAN security include:

- Decentralization through the use of DLTs can improve security by distributing control and minimizing single points of failure. [74,76,77,79–81,83].
- DLTs can offer features like transparency, immutability, traceability, and resiliency to create trustworthy and secure RAN environments [73–75,80,82–84].
- Distributed ledgers bring trust mechanisms for intrusion detection and authentication [73,74,76, 78,81–83].
- Using smart contracts on DLTs furthers resource planning, privacy control, and secure transactions in RAN environments [75,79,80].
- DLTs permit improvement of fault tolerance, performance, and scalability in RANs due to consensus algorithms [73–75,79–81,84].
- DLTs also can facilitate secure data sharing and traceability enhancement in RANs [73,80].

However, the listed disadvantages of using DLTs in RANs are summarized as follows:

- Consensus algorithms in DLTs can introduce communication overhead and impact network efficiency [73,76,80].

 doi:10.20944/preprints202504.2261.v1

- DLT-based architecture may increase implementation costs due to enhanced infrastructure and expertise [75,78,82,84].
- DLT brings scalability limitations that may harm, for example, throughput requirements and capacity of handling RAN operations [80,83,84].
- Consensus algorithms can insert into the RAN its weaknesses such as limitations in resisting certain attack models [81,84].
- Using DLTs in RANs provokes a trade-off between latency and security [74,80].

So, DLTs can offer relevant advantages in enhancing security and trust in RANs. However, it is necessary to consider the potential drawbacks such as communication overhead, complexity, scalability issues, and trade-offs between security and performance when implementing DLTs in RAN environments.

5.1.6. Future Work Suggestions

Future work suggestions emphasize the importance of further research in areas such as emerging technology integration, performance analysis, security enhancements, optimization, and practical testing of blockchain solutions in diverse network applications. The most recurring future work suggestions and topics considered for future study in the accepted papers include:

- Incorporating blockchain and IoT technologies in mobile networks with, for example, artificial intelligence techniques to accelerate towards decentralized networks in smart cities and other applications and analyzing the performance of blockchain/mobile network combination for improved efficiency and scalability [73,79,84].
- Developing analytical models to explore the characteristics of Blockchain Radio Access Networks in terms of latency, security, and other aspects to provide guidelines for real-world implementations, and evaluating performance, scalability, and security in different use cases [74,77,84].
- Testing Fronthaul security protocols with redundancy paths to identify better configurations [35,85–87].
- Testing isolation and authentication of network slicing [75,98,99].
- Improving RRC security issue identification tools [31,46,93–97].
- Testing authentication, encryption, and integrity over the wireless link in Femtocells [100].

Other future research topics include comparing alternative approaches to combining permissionless and permissioned elements in consensus algorithms [84], testing blockchain protocols in decentralized applications such as vehicle-to-everything (V2X) and wireless sensor networks (WSN) within access networks [77], and testing authentication, encryption, and integrity over the wireless links [100].

Moreover, future work can study advances in the application of Large Language Model (LLM) to increase RAN security, a topic that has been considered for different purposes, for example the management of radio resources in OpenRAN. [119].

5.2. Key Findings and Implications

The review was prepared chronologically to verify the items considered important by the academia over time. This way, it was possible to perceive that the academia turned its attention to the security of the Radio Resource Control (RRC) protocols in 2018 [46,93–95]. Among others, one of the concerns is that the RRC release can instruct the UE to re-select a cell, which could be used for redirection attacks to target a rogue base station for a downgrade attack.

The concern on RRC protocols security was overwhelmed by security within the Radio Access Network (RAN) edge at the turn of the decade, which led to the development of approaches using Distributed Ledger Technologies (DLTs), especially Blockchain, to increase security at the network edge [74–76,80–82]. Around the same time, in early 2021, there was an increase in interest in DLTs, as a technology company announced a significant purchase of bitcoins [120].

 doi:10.20944/preprints202504.2261.v1

There are different concerns about blockchain security since its adoption has been more frequently considered. This way, it is possible to infer that the use of DLTs, especially blockchain, addresses main network security issues, but brings its security vulnerabilities, as well as new attention points such as latency [73,77–79,83,84]. However, this review did not identify the use of DLTs other than blockchain applied to RANs.

Blockchain may raise latency concerns but be useful for less dynamic information security points, such as resource allocation. However, other DLTs may better deal with these issues, so further studies in this area are needed to confirm.

Nonetheless, some of the most recent works turned their attention to the security of RRC protocols again [31,96,97]. If, at the beginning of the evaluated period, RRC concerns focused on the vulnerability classes of process and operation and the security dimensions of access control and non-repudiation, in more recent works attention has turned to the vulnerability class of process and the security dimensions of access control and authentication.

5.2.1. Blockchain

5G technologies are a catalyzer to function decentralization, first from the core to the RAN, then to the edge, and decentralized networks (DNs). This decentralization is mainly encouraged by latency issues [113], which is highly influenced by resource allocation.

5G resource allocation process divvy up the network's resources among multiple users efficiently and fairly, and meets individual needs [114]. Resource allocation is integral to both user-facing and internal network management in 5G, so it includes radio spectrum, power, channeling, and Network Slicing, to name a few. While user-facing allocation ensures efficient delivery of services, internal allocation can customize and optimize the network infrastructure for diverse service needs, guaranteeing quality of service (QoS) and maximizing network efficiency.

The relationship between resource allocation and decentralization of network functions, and their influence on the QoS, especially latency, are the environment in which the accepted papers that study the application of blockchain in Radio Access Networks bloom. It is alleged the implementation of blockchain in RANs can improve resource-sharing efficiency and enhance network trust and security [74–76,80,82].

Nonetheless, the RAN Intelligent Controller (RIC) was introduced in the O-RAN Alliance specifications for providing control and management [121] by using artificial intelligence (AI) and analytics to enhance the access network. This way, a resource allocation scheme that supports latency requirements can be made available by the RIC [121–124]. A future research line can focus on comparing blockchain and AI/analytics applied to resource allocation.

Additionally, blockchain is considered to be used to implement IDS [81,83]. These works do not exhaust concerns about the latency and other QoS parameters. These papers study anomaly detection at the edge using different approaches, an edge blockchain that provides a secure and decentralized platform for data exchange and collaboration, and a machine learning/quantum computing decentralized environment that monitors network resources and builds trust between entrusted nodes, dedicated to optical network infrastructure. IDS/IPS systems are highlighted in Subsection 5.2.3.

However, the use of blockchain in RANs brings issues. The chain-based structure of this DLT and the use of a consensus algorithm and Sybil attack-resistance mechanism may introduce heavy communication traffic, which could affect QoS parameters, especially latency. DLTs have their vulnerabilities; blockchain, for instance, is susceptible to tampering and Sybil attacks. To face this matter, studied papers suggest solutions parallel to blockchain such as a tri-chain structure of blockchain [73]; an anonymous communication protocol [77]; the use of a Zero-Trust (ZT) security architecture [78]; data center-implemented artificial intelligence (AI) and big data [79]; quantum computing cryptanalysis through a federated blockchain model [83]; and mix of different consensus algorithms [84]. It is possible to note that the chronological approach to investigating blockchain-based improvements shows a transition in academia's concern over time, focusing on improving RANs by ledgering some

 doi:10.20944/preprints202504.2261.v1

network aspects, especially resource allocation, then showing that implementing blockchain in access networks brings its own vulnerabilities.

5.2.2. RRC

The vulnerabilities mentioned in the first papers [46,93–95] about Radio Resource Control security were access control and outdated assets. However, the most recent papers [31,96,97] indicate authentication and access control as the main vulnerabilities of RRC protocols. According to these articles, RRC protocols are vulnerable especially to bidding-down attacks, DDoS attacks, and MitM attacks. Bidding-down attacks aim, in general, to force a phone into a connection with an older generation to exploit legitimate protocol functionality, and allow them to eavesdrop on calls or text messages. Distributed Denial of Service (DDoS) is the tentative to flood the network servers to prevent users from accessing the network, online spots, or services. Man-in-the-Middle (MitM) is a class of attacks executed by the opponent to eavesdrop or impersonate one of the communication parties by positioning him or herself between the user and the application.

One of the main RRC features is the RRC connection release. Its message is used to command the RAN/UE connection release. The RRC connection release procedure with redirection information can also be used for re-selecting a cell in an older generation network, which makes all the mobile network generations, including 5G, prone to bidding-down attacks. This *generation downgrade* can be provoked by using a jammer to interfere with the frequency channel and force the UE to attach to another cell or another frequency channel used by an older generation. This action furthers the use of a rogue base station, for instance, to attract a UE into initiating a registration procedure, which can be used to perform MitM and DDoS attacks.

It is important to perceive that some works present security testing frameworks [31,46,95], which focus on identifying security issues, such as vulnerabilities. This way, further studies about the security improvement of RRC protocols are needed to develop proposals and tools.

5.2.3. IDS/IPS

The papers that investigate IDS and IPS consider, in general, Denial of Service (DoS) and Man-in-the-Middle (MitM) attacks as the most relevant risks. The proposed systems are anomaly-detection-based ones with different implementations. A network-based IDS (NIDS), that verifies whether traffic highly exceeds its normal amount and whether the exceeding time lasts long enough, is considered by a couple of papers [81,88].

Hybrid systems, that can merge different elements, are proposed as well. They are:

- a fault management module and a cyber-security management module [89];
- a pattern-detection, firewall, and IDS/IPS arrangement [90]; and
- a framework composed of a signature-based and an anomaly-based intrusion detection [91].

Blockchain-based systems, that have more specific goals, such as Edge Computing (EC)-based NIDS architecture using various monitored edge network datasets [81] and a machine learning and quantum computing decentralized environment that monitors network resources and builds trust between untrusted nodes, dedicated to optical network infrastructure [83], also make up the IDS/IPS set.

An IoT-oriented IDS focused on patterns classification to discover attacks [92] is also part of the proposed solutions. It is possible to perceive that the core of the identified systems is the anomaly-detection system, which could infer that this is an attention point for future research.

5.2.4. Fronthaul

The Fronthaul (FH) provides the connectivity between the RAN Radio Unit (RU), which implements the lower physical functions, and the RAN Distributed Unit (DU), which implements the higher physical functions. This information is divided into four planes, Control, User, Synchronization, and Management planes. The enhanced Common Public Radio Interface (eCPRI) interface is used

 doi:10.20944/preprints202504.2261.v1

between the RU and DU for radio control and user data since it is Ethernet-based, which has ubiquitous applications and enables different types of traffic.

The clear-text nature of the four cited planes and their direct encapsulation over Ethernet could expose the FH to different attacks. The most cited in the papers identified in this research that deal with Fronthaul security [35,85–87] is the Man-in-the-Middle attack, which could impersonate a legitimate synchronization message and inject a false clock into the network causing degradation of the time service, resulting in a Denial-of-Service of the network. To face the cited threats, the majority of these papers [35,86,87] suggest the adoption of the Media Access Control Security (MACSec) standard, which its features of authentication, integrity, confidentiality, and replay protection, satisfies the Fronthaul security requisites. However, it is highlighted that MACSec possesses implementation challenges to fulfill mandated Fronthaul requirements of latency, bandwidth, and synchronization accuracy. The remaining paper [85] suggests the adoption of the WireGuard. This solution is a communication protocol that implements encrypted virtual private networks (VPNs) and is designed to reach ease of use, high-speed performance, and low attack surface. It is important to note that this work does not evaluate the security itself, but focuses its value judgment on throughput and latency.

5.2.5. Network Slicing

Network Slicing is a recurrent feature in the accepted papers. In Subsection 5.2.1 we see that blockchain can improve the security of resource allocation, including Network Slicing. However, there are other papers [98,99] that study slicing security without the use of blockchain technology. These works cite DoS, MitM, and replay attacks as possible risks to Network Slicing. The proposals to enhance slicing security include a certificateless signature scheme based on a cryptographic tool to provide data integrity and identity authentication and the use of an enhanced Virtual Private Network (VPN), which can improve the security of Radio Access Networks by providing a secure and isolated communication channel between the 4G/5G core networks and the RAN.

6. Conclusions

This systematic literature review aimed to study findings about improving security in RANs and evaluating DLTs and other security mechanisms used in RANs. The RAN security evaluation is not a simple task since it is a complex telecommunications network element. This is made of different hardware and software modules, virtualized functions, and standardized and non-standardized interfaces, and it is accessible to external users.

Notwithstanding, cybersecurity is not a tight concept. A network cannot guarantee security since new threats and vulnerabilities are discovered 24/7. So, cybersecurity is a continuous process and involves different players, such as vendors, operators, and users. This way, it is necessary to apply various approaches to increase network security such as user education, access limiting, hardware, software, personnel training updates, technology development monitoring, user activity monitoring, and more.

One innovation in this review to help increase access network security was the definition of five RAN attack classes, in which we could identify the most relevant vulnerabilities and threats. Furthermore, we related the different attack classes to the accepted papers' subjects. Regardless of the subject, the open-air interface is a possible avenue for various attacks. To attack Radio Access Networks, adversaries can take advantage mainly of *access control*, *data storage*, and *lack or weakness of security mechanism* vulnerabilities and target a myriad of menaces, which we have classified following what is established by ITU-T Recommendation X.805. So, attackers' main threats identified in the accepted papers are *disclosure of information* and *interruption of services*, regardless of the attack class. Besides, according to ITU-T Recommendation X.805, and confirmed by accepted papers' analysis, *non-repudiation* security dimension is useful to help face all defined attack classes, but remembering that security in access networks needs to be thought of holistically.

In this review, we identified different approaches studied to enhance RAN security. Different interest points, such as RRC, Fronthaul, and resource allocation were cited in the investigated papers

 doi:10.20944/preprints202504.2261.v1

and received proposals to increase their security. Furthermore, we verified different suggestions, like blockchain and anomaly detection, to increase RAN security, which includes its components and interfaces between them. However, the accepted papers do not study proactive RAN security planning as much as threat mitigation and vulnerability detection. It is a challenge to academia but also an opportunity since concepts such as Security by Design, Zero Trust Architecture, and Decryption of Network Traffic could be considered to enhance security in access networks throughout their lifecycle.

As we have preluded, we investigate how various security mechanisms are studied to improve RAN security. To enhance Fronthaul security, it is proposed to implement a new security stage, which can be a security pattern (e.g., MACSec) or a communication protocol (e.g., WireGuard). For Network Slicing, a certificateless signature and VPN were proposed. Furthermore, different RRC concerns were raised since it has a relevant role in the RAN/UE connection. Papers studying RRC are focused on identifying security issues, such as vulnerabilities, so it is a challenge and an opportunity to dig deep into security enhancements for the RRC.

Blockchain also attracts attention in accepted papers. Our results show blockchain is the only DLT used to develop Radio Access Networks and its main goal is to manage resource allocation. Besides, it is recurrently considered to be used to implement IDS, especially through anomaly detection. However, blockchain use in RANs brings challenges, including latency.

Beyond summarizing and evaluating found vulnerabilities, threats, and security suggestions, this systematic literature review recognizes challenges and recommendations for future research. The use of DLTs other than blockchain is not explored in the accepted papers, so the role of these DLTs in resource allocation and IDS/IPS can be investigated. In the same way, a comparison between blockchain-based and RIC-based resource allocation in terms of security and latency requirements could considered for future work. Besides, DLTs that better deal with latency may take place in future studies to investigate increasing security in *access control*, one of the vulnerabilities most investigated in the accepted papers.

This review discusses and answers the defined research questions, as we can see in Section 5. We could identify distributed ledgers applied to increase resource sharing, intrusion detection, and intrusion prevention. It is important to highlight that consensus algorithms may help to ensure the integrity and security of transactions and communications in RANs. Nonetheless, our findings show that resource allocation is the main interest in applying DLTs on RANs, as shown in Subsection 5.2.1.

Furthermore, it is proposed the adoption of security protocols, frameworks to support SDN controllers, and super edge data center establishment to increase RAN security. These tools can be based on technologies like blockchain, artificial intelligence, and big data for full potential.

When we specifically study the use of DLTs applied to network security, the accepted papers bring some examples such as transparent resource allocation and transactions, better load balance, scalability, flexibility, and a decentralized environment for network monitoring.

So, DLT usage in radio access networks brings advantages, however, it also could insert challenges that need to be considered before its implementation. Positive points discussed in the accepted papers include distributing control, reducing single points of failure, offering transparency, immutability, traceability, resiliency, improvement of fault tolerance, and facilitating data sharing. Possible drawbacks may be communication overhead, network complexity, scalability issues, and trade-offs between security and performance.

Finally, the accepted papers present different proposals for future work. These include emerging technology integration, performance analysis, and practical testing of blockchain solutions. Among DLT solutions, it is cited comparing permissioned/permissionless-merged elements in consensus algorithms and testing DLT protocols in decentralized applications.

So, DLTs can improve RAN security, however, the studied papers show that the main usage of DLT in access networks is resource allocation. Nevertheless, other solutions can be applied to better secure RANs, including combined and customized solutions. To this end, it is necessary to address the drawbacks found in this review.

 doi:10.20944/preprints202504.2261.v1

Acknowledgments: The authors thank *Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes)* for partial financing of this work and the *Universidade Federal de Campina Grande (UFCG)* for academic and infrastructure support.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Methodology

This appendix exposes the methodology considered for this work. It includes the search strategy, selection criteria, data extraction process, and quality assessment methods.

Appendix A.1. Search Strategy

We used the Population, Intervention, Context, and Outcome (PICO) framework to delimit the scope of the papers selected for this systematic review since it can also guide in the search string definition[125]. Thus, the selected PICO terms are:

- *Population*: Radio Access Network, RAN, Open Radio Access Network, OpenRAN, Open RAN, Open-RAN, O-RAN.
- *Intervention*: Distributed Ledger Technology, Distributed Ledger, DLT, Security Mechanisms, IOTA, Blockchain, Distributed Consensus Ledger, Federated Ledger.
- *Context*: Security, Privacy, Confidentiality, Integrity, Trustworthiness, Protection, Availability.
- *Outcome*: Solution, Technique, Tool, Approach, Method, Mechanism, Advantage, Benefit, Positive Point, Disadvantage, Drawback, Negative Point.

Appendix A.2. Search String

We defined the search string based on the keywords and PICO terms (Subsection A.1), using the boolean operators (AND and OR) to link them, as follows:

(*Radio Access Network* **OR** *OpenRAN* **OR** *Open RAN* **OR** *Open-RAN* **OR** *O-RAN*)

AND

(*Distributed Ledger* **OR** *DLT* **OR** *Security Mechanisms* **OR** *IOTA* **OR** *Blockchain* **OR** *Distributed Consensus Ledger* **OR** *Federated Ledger*)

AND

(*Solution* **OR** *Technique* **OR** *Tool* **OR** *Approach* **OR** *Method* **OR** *Mechanism* **OR** *Advantage* **OR** *Benefit* **OR** *Positive Point* **OR** *Disadvantage* **OR** *Drawback* **OR** *Negative Point*)

AND

(*Security* **OR** *Privacy* **OR** *Confidentiality* **OR** *Integrity* **OR** *Trustworthiness* **OR** *Protection* **OR** *Availability*)

It is important to highlight that we avoided the term *RAN* since it is equal to the past tense of the verb *run*, which interferes with the search results.

Appendix A.3. Search Repositories

To search for relevant papers, we defined the scientific repositories listed in Table A1, which gather articles from different conferences and journals.

Table A1. Selected repositories.

Repository	URL
ACM Digital Library	https://dl.acm.org/
EI Compendex	https://www.engineeringvillage.com/
IEEE Digital Library	https://ieeexplore.ieee.org/
Scopus	https://www.scopus.com/
Springer Link	https://link.springer.com/

It is important to highlight that we conducted the online search in the repositories on September 15, 2023.

 doi:10.20944/preprints202504.2261.v1

Appendix A.4. Selection Criteria

We determine the selection criteria for exclusion and inclusion of papers. The exclusion criteria, which aim to eliminate works not relevant to the research, are duplicate results, white papers, short papers, papers that don't answer the research questions, papers about lower layers of interconnection, book chapters, master and PhD theses, papers not written in English, papers published before 2010, secondary and tertiary studies, and full content not available in the repositories. We have defined 2010 as the cutoff point since it is the beginning of the 4G network implementation [126]. As there is no complete break during the evolution of mobile networks, works that study 3G networks after the defined cutoff date were considered for this review.

As important as the exclusion criteria, we have the inclusion ones, which can improve the probability of selecting papers that can help answer the research questions. The defined inclusion criteria are papers published in journal and conference papers and results that answer the research questions.

Appendix A.5. Selection Procedure

To select relevant papers, we defined the following steps based on the selection criteria:

- Exclusion of duplicate papers.
- Exclusion of white papers, short papers, and book chapters.
- Exclusion of papers that don't answer the research questions.
- Exclusion of papers about lower layers of interconnection.
- Exclusion of master and PhD theses.
- Exclusion of papers not written in English.
- Exclusion of papers published before 2010.
- Exclusion of secondary and tertiary studies.
- Exclusion of papers not published in journal or conference papers.
- Exclusion of papers whose full content is not available.
- Exclusion of papers not related to the topics.
- Deep analysis of the remaining papers to identify irrelevant ones.

Appendix A.6. Quality Assessment

We defined the paper quality assessment to guarantee that the most relevant articles are considered for this work. To assess the quality of the selected documents, we established quality assessment questions to rate the papers and evaluated them by answering all the questions. The possible answers for each question are yes, partially, or no, and each of them is scored as follows:

- Yes = 1
- Partially = 0.5
- No = 0

Below, we list the quality assessment questions with a guideline for the answers:

- Has the paper been peer-reviewed and published in a reputable journal?
  - Only receives 1 if the paper was published in a vehicle with a minimum impact factor of 2.
- Is the methodology used in the paper appropriate and clearly explained?
  - Only receives 1 if the paper has a clear methodology and is well written.
- Does the paper provide a thorough and balanced review of the literature on RAN or DLTs?
  - Only receives 1 if the paper has a broad approach to evaluating the formal literature on RAN or DLTs.
- Are the research results presented and supported by the data?
  - Only receives 1 if the paper validates the results in a well-structured way.

 doi:10.20944/preprints202504.2261.v1

- Are the conclusions of the paper supported by the evidence presented?
  - Only receives 1 if the conclusion is coherent with the results and the argumentation.
- Are any potential limitations or biases in the research acknowledged and discussed?
  - Only receives 1 if the structure of the paper respects the scientific method.
- Does the paper contribute new and relevant information to the field of RAN or DLTs?
  - Only receives 1 if the paper is innovative.
- Are the references cited in the paper current and relevant to RAN or DLTs?
  - Only receives 1 if the paper is well-grounded, with good, related references.

The score range is from zero to eight, as there are eight quality assessment questions. Using this classification, we defined the quality level as follows:

- High quality, if the paper scored above 5.
- Medium quality, if the paper scored between 3.5 and 5.
- Low quality if the paper scored up to 3.

Appendix A.7. Data Extraction

We defined the following data to be extracted from the accepted papers:

- Title
- Authors
- Abstract
- Year
- Type of paper
- Conference/journal name
- Country(ies) where the research was carried out
- Number of pages
- Number of citations
- Quality
- Identified RAN threats
- DLT employment to enhance RANs
- Approaches to increase RAN security
- DLT usage to increase RAN security
- Pros and cons of DLT to improve RAN security
- Future work suggestions

Appendix B. General Results

This Systematic Literature Review selected 352 papers based on the defined search string. The first evaluation of these selected papers rejected 219 works. There were 62 duplicated articles from the different search repositories. So, 71 works underwent a more in-depth analysis, as shown in Figure A1. The deep analysis of the remaining papers resulted in 31 rejected and 39 accepted papers. One of them was classified as low quality. Figure A2 summarizes these findings.

From the 39 accepted articles, 18 were published in conference proceedings and 21 in journals. Figure A3 shows the source repositories of rejected and accepted articles. Authors from 25 countries contributed partially or completely to the accepted papers' elaboration, as shown in Figure A4. It is important to perceive that we considered the countries of all the papers' authors. We can also see in this figure which countries are most interested in this research topic.

 doi:10.20944/preprints202504.2261.v1

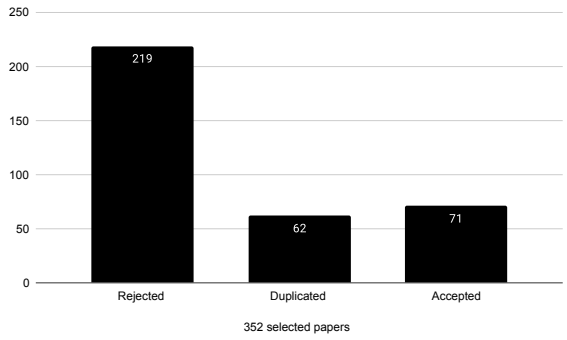

Figure A1. Selection from the search string.

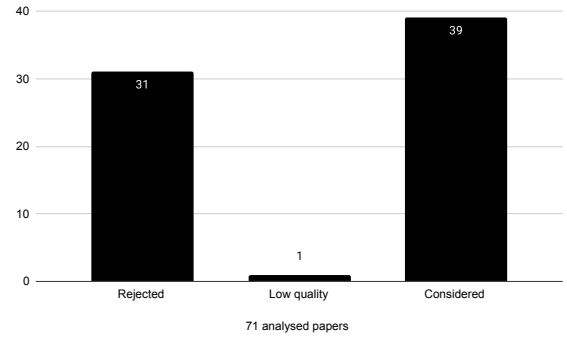

Figure A2. Paper acceptance after deep analysis.

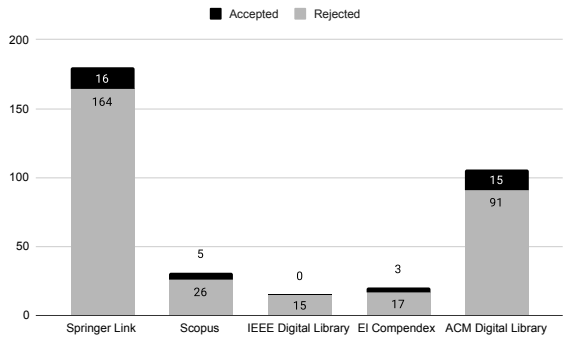

Figure A3. Source repositories of the papers.

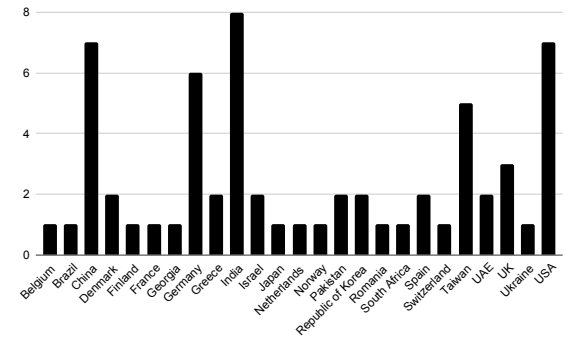

Figure A4. Geographic distribution of the authors.

We defined the start of the research as 2010 to coincide with the beginning of the implementation of 4G technology in mobile communications networks. However, the interest in the research topic has been increasing since the 2020s, as shown in Figure A5. It is important to note that we searched the

 doi:10.20944/preprints202504.2261.v1

digital repositories in September 2023, so maybe the year 2023 does not include the total work of the period.

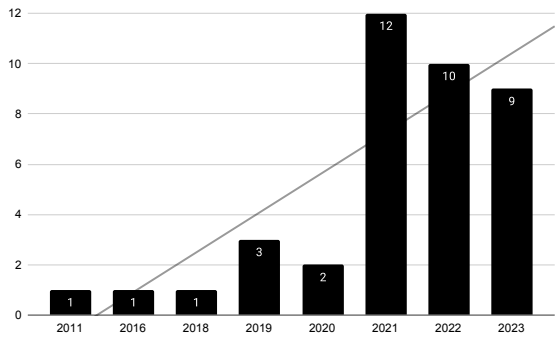

Figure A5. Number of accepted papers per year.

The 39 accepted papers sum 537 citations, and the average number of citations per paper is about 14. According to Figure A6, it is possible to verify that most papers have less than 12 citations, and only two were cited more than 58 times.

As we can see in Subsection A.6, the quality of the papers was ranked from 0 to 8. The paper is considered high quality if it scores above 5, medium quality between 3.5 and 5, and low quality up to 3. Among the evaluated works, only one was scored up to 3. Figure A7 shows the distribution of the quality assessment of the accepted papers. This histogram shows that, even among the 39 accepted papers, high-quality ones (score above 5) are the majority, which evidences these papers' relevance.

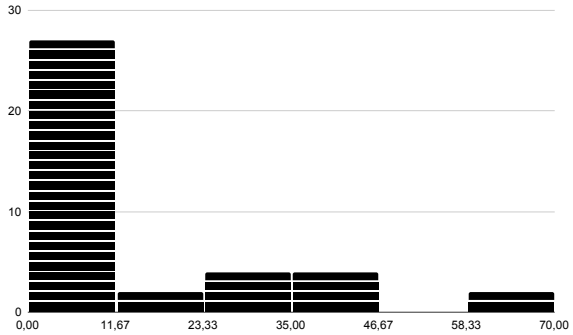

Figure A6. Number of citations for accepted papers.

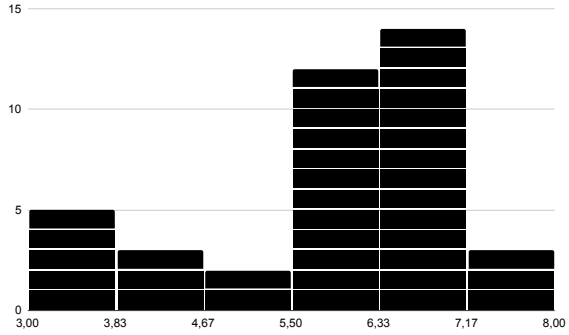

Figure A7. Quality score.

 doi:10.20944/preprints202504.2261.v1

References

1. Vivier, G. IoT: How 5G differs from LTE, 2021.
2. Olwal, T.O.; Djouani, K.; Kurien, A.M. A Survey of Resource Management Toward 5G Radio Access Networks. *IEEE Communications Surveys & Tutorials* **2016**, *18*, 1656–1686. https://doi.org/10.1109/COMST.2016.2550765.
3. Udell, C. 5G Security Concerns & Privacy Risks, 2023.
4. Firouzi, R.; Rahmani, R. Delay-sensitive resource allocation for IoT systems in 5G O-RAN networks. *Internet of Things* **2024**, *26*, 101131. https://doi.org/10.1016/j.iot.2024.101131.
5. ITU, I.T.U. Recommendation ITU-R M.2083-0 (09/2015) IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, 2015.
6. Condoluci, M.; Mahmoodi, T. Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges. *Computer Networks* **2018**, *146*, 65–84. https://doi.org/10.1016/j.comnet.2018.09.005.
7. hacen Diallo, E.; Agha, K.A.; Martin, S. TRADE-5G: A Blockchain-Based Transparent and Secure Resource Exchange for 5G Network Slicing. *Blockchain: Research and Applications* **2024**, p. 100246. https://doi.org/10.1016/j.bcra.2024.100246.
8. Alharbi, T.; Portmann, M. The (In)Security of Virtualization in Software Defined Networks. *IEEE Access* **2019**, *7*, 66584–66594. https://doi.org/10.1109/ACCESS.2019.2918101.
9. for Mobile Communications GSMA, G.S. 5G Security Issues. White paper, Global System for Mobile Communications - GSMA, 2019.
10. Hari Krishna, S.; Sharma, R. Survey on application programming interfaces in software defined networks and network function virtualization. *Global Transitions Proceedings* **2021**, *2*, 199–204. International Conference on Computing System and its Applications (ICCSA- 2021), https://doi.org/10.1016/j.gltp.2021.08.018.
11. National Telecommunications Agency. Resolution no. 740/2020, 2020.
12. Chaer, A.; Salah, K.; Lima, C.; Ray, P.P.; Sheltami, T. Blockchain for 5G: Opportunities and Challenges. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019; pp. 1–6. https://doi.org/10.1109/GCWkshps45667.2019.9024627.
13. Adib, D. What's blockchain got to do with edge computing?, 2023.
14. Kitchenham, B. Procedures for performing systematic reviews. *Keele, UK, Keele University* **2004**, *33*, 1–26.
15. Kitchenham, B.; Charters, S.; Budgen, D.; Brereton, P.; Turner, M.; Linkman, S.; Jørgensen, M.; Mendes, E.; Visaggio, G. Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, ver. 2.3 ebse technical report. ebse, 2007.
16. Houy, S.; Schmid, P.; Bartel, A. Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review. *ACM Computing Surveys* **2023**, *56*, 1–31. https://doi.org/10.1145/3596906.
17. Bachiega, J.; Costa, B.; Carvalho, L.R.; Rosa, M.J.F.; Araujo, A. Computational Resource Allocation in Fog Computing: A Comprehensive Survey. *ACM Comput. Surv.* **2023**, *55*. https://doi.org/10.1145/3586181.
18. Pooshideh, M.; Beheshti, A.; Qi, Y.; Farhood, H.; Simpson, M.; Gatland, N.; Soltany, M. Presentation Attack Detection: A Systematic Literature Review. *ACM Comput. Surv.* **2024**, *1*, 1–34. Just Accepted, https://doi.org/10.1145/3687264.
19. Mauri, L.; Cimato, S.; Damiani, E. A Comparative Analysis of Current Cryptocurrencies. In Proceedings of the ICISSP, 2018, pp. 127–138. https://doi.org/10.5220/0006648801270138.
20. Bencic, F.M.; Zarko, I.P. Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph. *CoRR* **2018**, *abs/1804.10013*, [1804.10013]. https://doi.org/10.48550/arXiv.1804.10013.
21. Yang, X.; Zhang, Y.; Wang, S.; Yu, B.; Li, F.; Li, Y.; Yan, W. LedgerDB: A Centralized Ledger Database for Universal Audit and Verification. *Proc. VLDB Endow.* **2020**, *13*, 3138–3151. https://doi.org/10.14778/3415478.3415540.
22. Shirey, R. RFC 4949: Internet Security Glossary, Version 2, 2007. https://doi.org/10.17487/RFC4949.
23. Group, N.C. ENISA Report on the cybersecurity of Open RAN, 2022.
24. Frank, W.; Rahman, A.; Daiekh, S.; Lee, J. Thinking like a 5G attacker: Leverage attack graphs to illuminate 5G network vulnerabilities, 2022.
25. ITU, I.T.U. Recommendation X.800 (03/91) Security architecture for open systems interconnection for CCITT applications, 1991.
26. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 3682–3722. https://doi.org/10.1109/COMST.2019.2916180.
27. ITU, I.T.U. Recommendation X.805 (10/03) Security architecture for systems providing end-to-end communications, 2003.

 doi:10.20944/preprints202504.2261.v1

28. 3GPP. 5G; NG-RAN; Architecture description (3GPP TS 38.401 version 15.10.0 Release 15). Technical Specification (TS) 38.401, 3rd Generation Partnership Project (3GPP), 2023. Version 15.10.0.
29. Singh, S.K.; Singh, R.; Kumbhani, B. The Evolution of Radio Access Network Towards Open-RAN: Challenges and Opportunities. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Seoul, South Korea, 2020; pp. 1–6. https://doi.org/10.1109/WCNCW48565.2020.9124820.
30. Prasad, R.; Prasad, A.R.; Mihovska, A.; Nidhi. *6G Enabling Technologies: New Dimensions to Wireless Communication*, 1 ed.; River Publishers: New York, 2022. https://doi.org/10.1201/9781003360889.
31. Erni, S.; Kotuliak, M.; Leu, P.; Roeschlin, M.; Capkun, S. AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. In Proceedings of the Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, New York, NY, USA, 2022; MobiCom '22, pp. 743–755. https://doi.org/10.1145/3495243.3560525.
32. Gonçalves, G.E.; Santos, G.L.; Ferreira, L.; Rocha, É.d.S.; de Souza, L.M.F.; Moreira, A.L.C.; Kelner, J.; Sadok, D., Flying to the Clouds: The Evolution of the 5G Radio Access Networks. In *The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing*; Springer International Publishing: Cham, 2020; chapter 3, pp. 41–60. https://doi.org/10.1007/978-3-030-41110-7_3.
33. Liu, C., Architectural Evolution and Novel Design of Fiber-Wireless Access Networks. In *Fiber-Wireless Convergence in Next-Generation Communication Networks*; Springer Cham: Cham, 2017; chapter 8, pp. 213—-233. https://doi.org/10.1007/978-3-319-42822-2_8.
34. America, A. Understanding Cable and Antenna Analysis, 2021.
35. Dik, D.; Berger, M.S. Open-RAN Fronthaul Transport Security Architecture and Implementation. *IEEE Access* **2023**, *11*, 46185–46203. https://doi.org/10.1109/ACCESS.2023.3274487.
36. Martin, D. Why do open RAN? | C-RAN, vRAN and open-RAN explained, 2023.
37. Polese, M.; Bonati, L.; D'Oro, S.; Basagni, S.; Melodia, T. Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges. *IEEE Communications Surveys & Tutorials* **2023**, *25*, 1376–1411. https://doi.org/10.1109/COMST.2023.3239220.
38. Yang, B.; Yang, X.; Ge, X.; Li, Q. Coverage and Handover Analysis of Ultra-Dense Millimeter-Wave Networks With Control and User Plane Separation Architecture. *IEEE Access* **2018**, *6*, 54739–54750. https://doi.org/10.1109/ACCESS.2018.2871363.
39. Da Silva, I.; Mildh, G.; Rune, J.; Wallentin, P.; Vikberg, J.; Schliwa-Bertling, P.; Fan, R. Tight Integration of New 5G Air Interface and LTE to Fulfill 5G Requirements. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Rio de Janeiro, Brazil, 05 2015; pp. 1–5. https://doi.org/10.1109/VTCSpring.2015.7146134.
40. Zeydan, E.; Mangues-Bafalluy, J.; Baranda, J.; Requena, M.; Turk, Y. Service Based Virtual RAN Architecture for Next Generation Cellular Systems. *IEEE Access* **2022**, *10*, 9455–9470. https://doi.org/10.1109/ACCESS.2022.3144534.
41. Sirotkin, S., Ed. *5G Radio Access Network Architecture: The Dark Side of 5G*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2020. https://doi.org/10.1002/9781119550921.
42. Kilinc, C.; Ericson, M.; Rugeland, P.; Da Silva, I.; Zaidi, A.; Aydin, O.; Venkatasubramanian, V.; Filippou, M.C.; Mezzavilla, M.; Kuruvatti, N.; et al. 5G Multi-RAT Integration Evaluations Using a Common PDCP Layer. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Glasglow, UK, 06 2017; pp. 1–5. https://doi.org/10.1109/VTCSpring.2017.8108594.
43. Shen, J.; Du, Z.; Zhang, Z.; Yang, N.; Tang, H., Eds. *5G NR and Enhancements*, 1 ed.; Elsevier: Radarweg 29, PO Box 211, 1000 AE Amsterdam, Netherlands, 2022. https://doi.org/10.1016/C2020-0-04150-2.
44. Barbuzzi, A.; Perala, P.H.; Boggia, G.; Pentikousis, K. 3GPP radio resource control in practice. *IEEE Wireless Communications* **2012**, *19*, 76–83. https://doi.org/10.1109/MWC.2012.6393521.
45. Potnuru, S.; Nakarmi, P.K. Berserker: ASN.1-based Fuzzing of Radio Resource Control Protocol for 4G and 5G. In Proceedings of the 2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Bologna, Italy, 10 2021; pp. 295–300. https://doi.org/10.1109/WiMob52687.2021.9606317.
46. Hussain, S.R.; Echeverria, M.; Karim, I.; Chowdhury, O.; Bertino, E. 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol. In Proceedings of the Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2019; CCS '19, p. 669–684. https://doi.org/10.1145/3319535.3354263.

 doi:10.20944/preprints202504.2261.v1

47. Mo, Y.; Cai, W.; Zhan, W.; Chen, Q.; Yin, Y.; Sun, X. Modeling and Performance Analysis of 5G RRC Protocol with Machine-Type Communications. In Proceedings of the 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 09 2022; pp. 475–480. https://doi.org/10.1109/PIMRC54779.2022.9977764.
48. Ayanampudi, H.; Dhuli, R. Performance analysis of Heterogeneous Cloud-Radio Access Networks: A user-centric approach with network scalability. *Computer Communications* **2022**, *194*, 202–212. https://doi.org/10.1016/j.comcom.2022.07.041.
49. Mateen, A.; Zhu, Q.; Afsar, S.; Rashid, W. Optimization of Fog Computing Based Radio Access Networks. In Proceedings of the Proceedings of the 7th International Conference on Software Engineering and New Technologies, New York, NY, USA, 2018; ICSENT 2018, pp. 1–8. https://doi.org/10.1145/3330089.3330120.
50. Rauchs, M.; Glidden, A.; Gordon, B.; Pieters, G.C.; Recanatini, M.; Rostand, F.; Vagneur, K.; Zhang, B.Z. Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN* **2018**. https://doi.org/10.2139/ssrn.3230013.
51. Zhelezov, D. PoW, PoS and DAGs are NOT consensus protocols, 2018.
52. Beyer, S. Proof-of-Work is not a Consensus Protocol: Understanding the Basics of Blockchain Consensus, 2019.
53. Bains, P. Blockchain Consensus Mechanisms: A Primer For Supervisors. Technical report, International Monetary Fund, 2022. NOTE/2022/003, https://doi.org/10.5089/9781616358280.063.
54. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 1432–1465. https://doi.org/10.1109/COMST.2020.2969706.
55. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), 06 2017, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85.
56. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Transactions on Industrial Informatics* **2020**, *16*, 4177–4186. https://doi.org/10.1109/TII.2019.2942190.
57. Chowdhury, M.J.M.; Ferdous, M.S.; Biswas, K.; Chowdhury, N.; Kayes, A.S.M.; Alazab, M.; Watters, P. A Comparative Analysis of Distributed Ledger Technology Platforms. *IEEE Access* **2019**, *7*, 167930–167943. https://doi.org/10.1109/ACCESS.2019.2953729.
58. Kuhn, R.; Yaga, D.; Voas, J. Rethinking Distributed Ledger Technology. *Computer* **2019**, *52*, 68–72. https://doi.org/10.1109/MC.2019.2898162.
59. Moussaoui, M.; Aryal, N.; Bertin, E.; Crespi, N. Distributed Ledger Technologies for Cellular Networks and Beyond 5G: a survey. In Proceedings of the 2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 09 2022, pp. 37–44. https://doi.org/10.1109/BRAINS55737.2022.9908598.
60. Estrada, C.A.; Naranjo, S.S.; Toasa, V.J.; Yoo, S.G. A Systematic Literature Review of Blockchain Technology: Applications Fields, Platforms, and Consensus Protocols. In Proceedings of the Proceedings of the 2023 7th International Conference on Computer Science and Artificial Intelligence, New York, NY, USA, 2024; CSAI '23, p. 123–131. https://doi.org/10.1145/3638584.3638632.
61. Lashkari, B.; Musilek, P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. https://doi.org/10.1109/ACCESS.2021.3065880.
62. Lamport, L. Generalized Consensus and Paxos. *Microsoft Research Technical Report MSR-TR-2005-33* **2004**.
63. Bastiaan, M. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin (2015). In Proceedings of the Twente Student Conference on IT, 2021, pp. 1–10.
64. Sanda, O.; Pavlidis, M.; Seraj, S.; Polatidis, N. Long-Range attack detection on permissionless blockchains using Deep Learning. *Expert Systems with Applications* **2023**, *218*, 119606. https://doi.org/10.1016/j.eswa.2023.119606.
65. Dutta, A.; Hammad, E. 5G Security Challenges and Opportunities: A System Approach. In Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 109–114. https://doi.org/10.1109/5GWF49715.2020.9221122.
66. Zhang, S. An Overview of Network Slicing for 5G. *IEEE Wireless Communications* **2019**, *26*, 111–117. https://doi.org/10.1109/MWC.2019.1800234.
67. Habibi, M.A.; Nasimi, M.; Han, B.; Schotten, H.D. A Comprehensive Survey of RAN Architectures Toward 5G Mobile Communication System. *IEEE Access* **2019**, *7*, 70371–70421. https://doi.org/10.1109/ACCESS.2019.2919657.

 doi:10.20944/preprints202504.2261.v1

68. Toh, C.K. *Wireless ATM and Ad-Hoc Networks: Protocols and Architectures*; Springer: New York, NY, 1997. https://doi.org/10.1007/978-1-4615-6307-5.
69. Bandara, H.; Jayasumana, A. Collaborative applications over peer-to-peer systems–challenges and solutions. *Peer-to-Peer Network Applications* **2013**. https://doi.org/10.1007/s12083-012-0157-3.
70. Shaikh, F.S.; Wismüller, R. Routing in Multi-Hop Cellular Device-to-Device (D2D) Networks: A Survey. *IEEE Communications Surveys & Tutorials* **2018**, pp. 2622–2657. https://doi.org/10.1109/COMST.2018.2848108.
71. Verma, P.K.; Verma, R.; Prakash, A.; Agrawal, A.; Naik, K.; Tripathi, R.; Alsabaan, M.; Khalifa, T.; Abdelkader, T.; Abogharaf, A. Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications* **2016**, pp. 83–105. https://doi.org/10.1016/j.jnca.2016.02.016.
72. Safavat, S.; Sapavath, N.N.; Rawat, D.B. Recent advances in mobile edge computing and content caching. *Digital Communications and Networks* **2020**, *6*, 189–194. https://doi.org/10.1016/j.dcan.2019.08.004.
73. Tong, W.; Dong, X.; Shen, Y.; Zheng, J. BC-RAN: Cloud radio access network enabled by blockchain for 5G. *Computer Communications* **2020**, *162*, 179–186. https://doi.org/10.1016/j.comcom.2020.08.020.
74. Wang, J.; Ling, X.; Le, Y.; Huang, Y.; You, X. Blockchain-enabled wireless communications: a new paradigm towards 6G. *National Science Review* **2021**, *8*, nwab069, [https://academic.oup.com/nsr/article-pdf/8/9/nwab069/40377479/nwab069.pdf]. https://doi.org/10.1093/nsr/nwab069.
75. Gonçalves, J.P.d.B.; de Resende, H.C.; Villaca, R.d.S.; Municio, E.; Both, C.B.; Marquez-Barja, J.M. Distributed network slicing management using blockchains in E-health environments. *Mobile Networks and Applications* **2021**, *26*, 2111–2122. https://doi.org/10.1007/s11036-021-01745-1.
76. Valero, J.M.J.; Sánchez, P.M.S.; Lekidis, A.; Hidalgo, J.F.; Pérez, M.G.; Siddiqui, M.S.; Celdrán, A.H.; Pérez, G.M. Design of a Security and Trust Framework for 5G Multi-domain Scenarios. *Journal of Network and Systems Management* **2022**, *30*, 1–35. https://doi.org/10.1007/s10922-021-09623-7.
77. Ling, X.; Chen, P.; Wang, J.; Ding, Z. Data Broker: Dynamic Multi-Hop Routing Protocol in Blockchain Radio Access Network. *IEEE Communications Letters* **2021**, *25*, 4000–4004. https://doi.org/10.1109/LCOMM.2021.3114218.
78. Li, S.; Iqbal, M.; Saxena, N. Future Industry Internet of Things with Zero-trust Security. *Information Systems Frontiers* **2022**, *1*, 1–14. https://doi.org/10.1007/s10796-021-10199-5.
79. S, V.; Manoharan, R.; Ramachandran, S.; Rajasekar, V. Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 4868–4874. https://doi.org/10.1109/TII.2021.3107556.
80. Wang, Z.; Cao, B.; Liu, C.; Xu, C.; Zhang, L. Blockchain-based fog radio access networks: Architecture, key technologies, and challenges. *Digital Communications and Networks* **2022**, *8*, 720–726. https://doi.org/10.1016/j.dcan.2021.12.006.
81. Pandey, B.K.; Saxena, V.; Barve, A.; Bhagat, A.K.; Devi, R.; Gupta, R. Evaluation of soft computing in intrusion detection for secure social Internet of Things based on collaborative edge computing. *Soft Computing* **2023**, *1*, 1–11. https://doi.org/10.1007/s00500-023-08397-1.
82. Le, Y.; Ling, X.; Wang, J.; Guo, R.; Huang, Y.; Wang, C.X.; You, X. Resource Sharing and Trading of Blockchain Radio Access Networks: Architecture and Prototype Design. *IEEE Internet of Things Journal* **2023**, *10*, 12025–12043. https://doi.org/10.1109/JIOT.2021.3135414.
83. Wang, F.; Liao, S.; Yin, Y.; Ni, R.; Zhang, Y. Radio optical network security analysis with routing in quantum computing for 5G wireless communication using blockchain machine learning model. *Optical and Quantum Electronics* **2023**, *55*, 1–16. https://doi.org/10.1007/s11082-023-05277-8.
84. Tang, Y.; Yan, J.; Chakraborty, C.; Sun, Y. Hedera: A Permissionless and Scalable Hybrid Blockchain Consensus Algorithm in Multiaccess Edge Computing for IoT. *IEEE Internet of Things Journal* **2023**, *10*, 21187–21202. https://doi.org/10.1109/JIOT.2023.3279108.
85. Cho, J.Y.; Sergeev, A.; Zou, J. Securing Ethernet-based Optical Fronthaul for 5G Network. In Proceedings of the Proceedings of the 14th International Conference on Availability, Reliability and Security, New York, NY, USA, 2019; ARES '19, pp. 1–6. https://doi.org/10.1145/3339252.3341484.
86. Cho, J.Y.; Sergeev, A. Secure Open Fronthaul Interface for 5G Networks. In Proceedings of the Proceedings of the 16th International Conference on Availability, Reliability and Security, New York, NY, USA, 2021; ARES '21, pp. 1–6. https://doi.org/10.1145/3465481.3470080.
87. Dik, D.; Berger, M.S. Transport Security Considerations for the Open-RAN Fronthaul. In Proceedings of the 2021 IEEE 4th 5G World Forum (5GWF), Los Alamitos, US, 2021; pp. 253–258. https://doi.org/10.1109/5GWF52925.2021.00051.

 doi:10.20944/preprints202504.2261.v1

88. Chiu, S.T.; Leu, F.Y. Detecting DoS and DDoS Attacks by Using CuSum Algorithm in 5G Networks. In Proceedings of the Advances in Networked-Based Information Systems; Barolli, L.; Li, K.F.; Enokido, T.; Takizawa, M., Eds., Cham, 2021; pp. 1–9. https://doi.org/10.1007/978-3-030-57811-4_1.
89. Benslimen, Y.; Sedjelmaci, H.; Manenti, A.C. Attacks and failures prediction framework for a collaborative 5G mobile network, 2021. https://doi.org/10.1007/s00607-020-00893-8.
90. Iavich, M.; Gnatyuk, S.; Odarchenko, R.; Bocu, R.; Simonov, S. The Novel System of Attacks Detection in 5G. In Proceedings of the Advanced Information Networking and Applications; Barolli, L.; Woungang, I.; Enokido, T., Eds., Cham, 2021; pp. 580–591. https://doi.org/10.1007/978-3-030-75075-6_47.
91. Singh, A.; Chatterjee, K.; Satapathy, S. An edge based hybrid intrusion detection framework for mobile edge computing. In Proceedings of the Complex & Intelligent Systems, Cham, 2021; pp. 3719—3746. https://doi.org/10.1007/s40747-021-00498-4.
92. Jeyaselvi, M.; Dhanaraj, R.K.; Sathya, M.; Memon, F.H.; Krishnasamy, L.; Dev, K.; Ziyue, W.; Qureshi, N.M.F. A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks. *Cluster Computing* **2023**, *26*, 559–574. https://doi.org/10.1007/s10586-022-03607-1.
93. Saxena, N.; Grijalva, S.; Chaudhari, N.S. Authentication Protocol for an IoT-Enabled LTE Network. *ACM Trans. Internet Technol.* **2016**, *16*. https://doi.org/10.1145/2981547.
94. Shaik, A.; Borgaonkar, R.; Park, S.; Seifert, J.P. On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks. In Proceedings of the Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, 2018; WiSec '18, p. 75–86. https://doi.org/10.1145/3212480.3212497.
95. Chlosta, M.; Rupprecht, D.; Holz, T.; Pöpper, C. LTE Security Disabled: Misconfiguration in Commercial Networks. In Proceedings of the Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, 2019; WiSec '19, pp. 261—266. https://doi.org/10.1145/3317549.3324927.
96. Bitsikas, E.; Khandker, S.; Salous, A.; Ranganathan, A.; Piqueras Jover, R.; Pöpper, C. UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework. In Proceedings of the Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, 2023; WiSec '23, pp. 121—-132. https://doi.org/10.1145/3558482.3590194.
97. Karakoc, B.; Fürste, N.; Rupprecht, D.; Kohls, K. Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G. In Proceedings of the Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, 2023; WiSec '23, pp. 97—-108. https://doi.org/10.1145/3558482.3581774.
98. Huang, J.J.; Fan, C.I.; Hsu, Y.C.; Karati, A. A Fast Authentication Scheme for Cross-Network-Slicing Based on Multiple Operators in 5G Environments. In Proceedings of the Security in Computing and Communications; Thampi, S.M.; Wang, G.; Rawat, D.B.; Ko, R.; Fan, C.I., Eds., Singapore, 2021; pp. 92–106. https://doi.org/10.1007/978-981-16-0422-5_7.
99. Dzogovic, B.; Mahmood, T.; Santos, B.; Feng, B.; Do, V.T.; Jacot, N.; Van Do, T. Advanced 5g network slicing isolation using enhanced vpn+ for healthcare verticals. In Proceedings of the Smart Objects and Technologies for Social Good: 7th EAI International Conference, GOODTECHS 2021, Virtual Event, September 15–17, 2021, Proceedings 7, Cham, 2021; pp. 121–135. https://doi.org/10.1007/978-3-030-91421-9_10.
100. Borgaonkar, R.; Redon, K.; Seifert, J.P. Security Analysis of a Femtocell Device. In Proceedings of the Proceedings of the 4th International Conference on Security of Information and Networks, New York, NY, USA, 2011; SIN '11, p. 95–102. https://doi.org/10.1145/2070425.2070442.
101. Wang, S.; Tu, G.H.; Lei, X.; Xie, T.; Li, C.Y.; Chou, P.Y.; Hsieh, F.; Hu, Y.; Xiao, L.; Peng, C. Insecurity of Operational Cellular IoT Service: New Vulnerabilities, Attacks, and Countermeasures. In Proceedings of the Proceedings of the 27th Annual International Conference on Mobile Computing and Networking, New York, NY, USA, 2021; MobiCom '21, p. 437–450. https://doi.org/10.1145/3447993.3483239.
102. Chen, H.Y.; Rao, S.P. Adversarial trends in mobile communication systems: from attack patterns to potential defenses strategies. In Proceedings of the Secure IT Systems: 26th Nordic Conference, NordSec 2021, Virtual Event, November 29–30, 2021, Proceedings 26, Springer, Tampere, FI, 2021; pp. 153–171. https://doi.org/10.1007/978-3-030-91625-1_9.
103. Ahmed, A.; Qureshi, K.N.; Anwar, M.; Masud, F.; Imtiaz, J.; Jeon, G. Link-based penalized trust management scheme for preemptive measures to secure the edge-based internet of things networks. *Wireless Networks* **2022**, *30*, 1–23. https://doi.org/10.1007/s11276-022-02948-4.

 doi:10.20944/preprints202504.2261.v1

104. Pamarthi, S.; Narmadha, R. Intelligent privacy preservation proctol in wireless MANET for IoT applications using hybrid crow search-harris hawks optimization. *Wireless Networks* **2022**, *28*, 2713–2729. https://doi.org/10.1007/s11276-022-02986-y.
105. Lekidis, A. Cyber-Security Measures for Protecting EPES Systems in the 5G Area. In Proceedings of the Proceedings of the 17th International Conference on Availability, Reliability and Security, New York, NY, USA, 2022; ARES '22, pp. 1–10. https://doi.org/10.1145/3538969.3544476.
106. Hu, Y.; Chen, M.Y.; Tu, G.H.; Li, C.Y.; Wang, S.; Shi, J.; Xie, T.; Xiao, L.; Peng, C.; Tan, Z.; et al. Uncovering Insecure Designs of Cellular Emergency Services (911). In Proceedings of the Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, New York, NY, USA, 2022; MobiCom '22, p. 703–715. https://doi.org/10.1145/3495243.3560534.
107. Reshma, G.; Prasanna, B.; Murthy, H.; Murthy, T.; Parthiban, S.; Sangeetha, M. Privacy-aware access control (PAAC)-based biometric authentication protocol (Bap) for mobile edge computing environment. *Soft Computing* **2023**, *1*, 1–20. https://doi.org/10.1007/s00500-023-08226-5.
108. Hu, Y.; Chen, M.Y.; Tu, G.H.; Li, C.Y.; Wang, S.; Shi, J.; Xie, T.; Xiao, L.; Peng, C.; Tan, Z.; et al. Unveiling the Insecurity of Operational Cellular Emergency Services (911): Vulnerabilities, Attacks, and Countermeasures. *GetMobile: Mobile Comp. and Comm.* **2023**, *27*, 39–43. https://doi.org/10.1145/3599184.3599195.
109. Valadares, D.; Will, N.; Sobrinho, Á.; Lima, A.; Morais, I.; Santos, D. Systematic Literature Review on 5G-IoT Security Aspects. *Preprints* **2023**, *1*, 1–34. https://doi.org/10.20944/preprints202311.0565.v1.
110. Zhuang, T.; Lin, Z. The why, what, and how of AI-based coding in scientific research, 2024, [arXiv:cs.CY/2410.02156]. https://doi.org/10.48550/arXiv.2410.02156.
111. Corporation, I. Cost of a Data Breach Report 2024, 2024.
112. Landi, M. Global IT outage knocks airlines, banks and others offline, 2024.
113. Sarah, A.; Nencioni, G.; Khan, M.M.I. Resource Allocation in Multi-access Edge Computing for 5G-and-beyond networks. *Computer Networks* **2023**, *227*, 109720. https://doi.org/10.1016/j.comnet.2023.109720.
114. Kamal, M.A.; Raza, H.W.; Alam, M.M.; Su'ud, M.M.; Sajak, A.b.A.B. Resource allocation schemes for 5G network: A systematic review. *Sensors* **2021**, *21*, 6588. https://doi.org/10.3390/s21196588.
115. Chen, Y.Z.; Chen, T.Y.H.; Su, P.J.; Liu, C.T. A Brief Survey of Open Radio Access Network (O-RAN) Security, 2023, [arXiv:cs.NI/2311.02311]. https://doi.org/10.48550/arXiv.2311.02311.
116. Mimran, D.; Bitton, R.; Kfir, Y.; Klevansky, E.; Brodt, O.; Lehmann, H.; Elovici, Y.; Shabtai, A. Security of Open Radio Access Networks. *Computers & Security* **2022**, *122*, 102890. https://doi.org/10.1016/j.cose.2022.102890.
117. Olsson, J.; Shorov, A.; Abdelrazek, L.; Whitefield, J. Zero trust and 5G – Realizing zero trust in networks, 2021.
118. Costlow, J. How Decryption of Network Traffic Can Improve Security, 2021.
119. Wu, X.; Farooq, J.; Wang, Y.; Chen, J. LLM-xApp: A Large Language Model Empowered Radio Resource Management xApp for 5G O-RAN. In Proceedings of the Symposium on Networks and Distributed Systems Security (NDSS), Workshop on Security and Privacy of Next-Generation Networks (FutureG 2025), San Diego, CA, 2025.
120. Randewich, N. Musk's bitcoin bet fuels gains in companies already invested, 2021.
121. Wang, Q.; Liu, Y.; Wang, Y.; Xiong, X.; Zong, J.; Wang, J.; Chen, P. Resource Allocation Based on Radio Intelligence Controller for Open RAN Toward 6G. *IEEE Access* **2023**, *11*, 97909–97919. https://doi.org/10.1109/ACCESS.2023.3311888.
122. Singh, A.K.; Khoa Nguyen, K. Joint Selection of Local Trainers and Resource Allocation for Federated Learning in Open RAN Intelligent Controllers. In Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), 2022, pp. 1874–1879. https://doi.org/10.1109/WCNC51071.2022.9771700.
123. Arnaz, A.; Lipman, J.; Abolhasan, M.; Hiltunen, M. Toward Integrating Intelligence and Programmability in Open Radio Access Networks: A Comprehensive Survey. *IEEE Access* **2022**, *10*, 67747–67770. https://doi.org/10.1109/ACCESS.2022.3183989.
124. Abdalla, A.S.; Upadhyaya, P.S.; Shah, V.K.; Marojevic, V. Toward Next Generation Open Radio Access Networks: What O-RAN Can and Cannot Do! *IEEE Network* **2022**, *36*, 206–213. https://doi.org/10.1109/MNET.108.2100659.

 doi:10.20944/preprints202504.2261.v1

125. Eldawlatly, A.; Alshehri, H.; Alqahtani, A.; Ahmad, A.; Al-Dammas, F.; Marzouk, A. Appearance of Population, Intervention, Comparison, and Outcome as research question in the title of articles of three different anesthesia journals: A pilot study. *Saudi Journal of Anaesthesia* **2018**, *12*, 175–177. https://doi.org/10.4103/sja.SJA_767_17.
126. Acharya, S.; Petrin, G. ITU World Radiocommunication Seminar highlights future communication technologies, 2010.