future internet

MDPI

Review

Understanding Security Vulnerabilities in Private 5G Networks: Insights from a Literature Review

Jacinta Fue [1], Jairo A. Gutierrez [1,*] and Yezid Donoso [2]

[1] Department of Computer and Information Sciences, School of Engineering, Computer, and Mathematical Sciences, Auckland University of Technology, Auckland 1010, New Zealand
[2] Department of Systems and Computing Engineering, Faculty of Engineering, Universidad de los Andes, Bogotá 111711, Colombia; ydonoso@uniandes.edu.co
* Correspondence: jairo.gutierrez@aut.ac.nz

Abstract

Private fifth generation (5G) networks have emerged as a cornerstone for ultra-reliable, low-latency connectivity across mission-critical domains such as industrial automation, healthcare, and smart cities. Compared to conventional technologies like 4G or Wi-Fi, they provide clear advantages, including enhanced service continuity, higher reliability, and customizable security controls. However, these benefits come with new security challenges, particularly regarding the confidentiality, integrity, and availability of data and services. This article presents a review of security vulnerabilities in private 5G networks. The review pursues four objectives: (i) to identify and categorize key vulnerabilities, (ii) to analyze threats that undermine core security principles, (iii) to evaluate mitigation strategies proposed in the literature, and (iv) to outline gaps that demand further investigation. The findings offer a structured perspective on the evolving threat landscape of private 5G networks, highlighting both well-documented risks and emerging concerns. By mapping vulnerabilities to mitigation approaches and identifying areas where current solutions fall short, this study provides critical insights for researchers, practitioners, and policymakers. Ultimately, the review underscores the urgent need for robust and adaptive security frameworks to ensure the resilience of private 5G deployments in increasingly complex and high-stakes environments.

Keywords: private 5G networks; Non-Public 5G Networks (NPNs); Standalone Non-Public Networks (SNPNs); 5G security challenges; security vulnerabilities in private 5G networks

Academic Editors: Mario Di Mauro and Francesco Pascale

Received: 29 September 2025
Revised: 17 October 2025
Accepted: 20 October 2025
Published: 23 October 2025

Citation: Fue, J.; Gutierrez, J.A.; Donoso, Y. Understanding Security Vulnerabilities in Private 5G Networks: Insights from a Literature Review. *Future Internet* **2025**, *17*, 485. https://doi.org/10.3390/fi17110485

1. Introduction

The rapid advancement of emerging technologies, particularly in cloud computing, has transformed both public and private sectors, creating unprecedented demand for communication infrastructures capable of higher data rates, lower latency, and greater reliability [1]. Simultaneously, the frequency and sophistication of cyberattacks have escalated, targeting critical industries such as healthcare and finance [2]. In healthcare, for instance, security breaches can result in catastrophic consequences, ranging from the exposure of sensitive patient data to the disruption of essential medical services [3]. Ransomware incidents may compromise electronic health records, delaying treatment and endangering lives, while also generating substantial financial and reputational costs for affected organizations, including legal disputes, recovery expenses, and the implementation of additional safeguards [4].

The introduction of 5G has created new opportunities for ultra-reliable, low-latency communication across sectors such as industrial automation, healthcare, and smart cities [5]. Yet, 5G infrastructures also face notable security risks, including Distributed Denial of Service (DDoS) and jamming attacks, which threaten critical network functions such as slicing and radio access [6]. Further vulnerabilities stem from weaknesses in authentication mechanisms [7,8] and the resource constraints of IoT devices, which often limit the implementation of robust encryption and integrity protections [4].

Private 5G networks, also referred to as Non-Public Networks (NPNs), enable organizations to deploy dedicated infrastructures with greater autonomy over security policies, data management, and service configurations [9]. Compared to public networks, private 5G offers advantages such as enhanced indoor coverage, tailored reliability, and improved protection of sensitive information [10]. However, these benefits are counterbalanced by emerging challenges. Expanded attack surfaces introduced by IoT integration, edge computing, and network slicing—combined with the coexistence of legacy systems and insider threats—amplify the risks of unauthorized access, operational disruptions, and data exfiltration [8,10].

The advent of Industry 4.0 and the rapid proliferation of the Internet of Things (IoT) have intensified the demand for advanced connectivity solutions capable of supporting massive device deployments, ultra-low latency, and high reliability [11]. Private 5G networks, also referred to as non-public networks (NPNs), have emerged as a strategic response to these demands, providing enterprises with dedicated and secure connectivity tailored to specific operational requirements [5]. Unlike public 5G networks, which serve multiple users under mobile network operators (MNOs), private 5G delivers exclusive infrastructure for a single organization, making it particularly advantageous in mission-critical environments such as manufacturing plants, hospitals, airports, ports, and defense facilities.

Private 5G networks offer organizations enhanced control over their infrastructure, allowing customization of security policies, quality-of-service parameters, and network configurations. Two primary deployment models are widely adopted: independent private 5G, fully owned and managed by the enterprise or a system integrator, and dependent private 5G, operated by an MNO that provides infrastructure, spectrum, and ongoing maintenance [9,12]. While the independent model delivers maximum autonomy and security, it demands substantial investment and technical expertise. Conversely, the dependent model lowers operational burdens but may introduce concerns regarding data privacy and control.

Problem Statement: despite their growing adoption in mission-critical sectors such as healthcare, manufacturing, and smart cities, the security of private 5G networks remains insufficiently addressed in the current body of research. Most studies emphasize public 5G infrastructures, leaving a gap in understanding the unique vulnerabilities of private deployments. This lack of targeted investigation limits the development of robust security frameworks and exposes organizations to heightened risks, including unauthorized access, operational downtime, and large-scale data breaches. To address this gap, this study conducts a literature review with four primary goals:

(i) To identify and categorize the main security vulnerabilities in private 5G networks;
(ii) To analyze risks affecting data confidentiality, integrity, and availability;
(iii) To examine mitigation strategies proposed in the literature;
(iv) To highlight gaps and opportunities for future research.

Together, these questions structure the review and ensure a comprehensive understanding of the vulnerabilities, threats, and countermeasures relevant to private 5G security.

2. Literature Review

2.1. Background

Private 5G adoption is accelerating due to its ability to ensure secure, low-latency, and highly reliable communication. In healthcare, it enables safe transmission of patient data, telemedicine services, and even remote surgeries [13]. In manufacturing, it underpins smart factories through real-time monitoring and predictive maintenance. For ports, campuses, and smart cities, private 5G guarantees scalable and resilient connectivity [14]. Table 1 summarizes the main application sectors and their connectivity, security, and efficiency benefits.

Table 1. Private 5G Networks Across Different Industries.

Industry/Organisation	Purpose of Private 5G Network	Key Applications
Manufacturing Plants	Enhance automation and IoT	Smart factories, real-time monitoring, robotics
Ports	Improve logistics and operations	Shipment tracking, automation
Smart Cities	Manage infrastructure, public services	Autonomous vehicles, traffic control, smart grids
Healthcare	Support telemedicine and data security	Remote monitoring, telemedicine, secure data transmission
Educational Campuses	Provide secure, high-speed internet	VR/AR applications, remote learning
Energy and Utility	Monitor and control infrastructure	Smart grids, predictive maintenance
Logistics and Supply Chain	Improve tracking and automation	Asset tracking, warehouse automation
Financial Institutions	Ensure secure and fast transactions	Real-time data analysis, compliance with data protection
Airports	Optimize operations and communications	Baggage handling, real-time data for security
Retail	Enhance customer experience and operations	Smart stores, contactless payments, inventory management

Note. Data collected and gathered from various articles used for thesis. All authors are cited accordingly.

Looking forward, the integration of AI-driven network management and edge computing is expected to enhance automation, adaptability, and operational efficiency within private 5G networks, enabling more sophisticated applications and laying the groundwork for future 6G innovations [15].

2.2. Architecture of Private 5G Networks

Private 5G networks consist of three fundamental components: the Radio Access Network (RAN), the core network, and user equipment (UE). The RAN, comprising base stations and antennas, facilitates wireless connectivity between devices and the network, ensuring seamless communication and high data throughput. The core network manages device mobility, routing, and enforces security policies, guaranteeing the confidentiality, integrity, and availability of network services [16]. User equipment—including smartphones, tablets, and IoT devices—interfaces with both the RAN and core network to enable reliable and low-latency communication [17]. Collectively, these elements provide a foundation for high-performance, flexible, and secure private 5G deployments tailored to organizational requirements.

Private 5G networks support multiple deployment models, primarily standalone (SA) and non-standalone (NSA) configurations [8]. Standalone networks operate independently from public infrastructures, granting organizations full control over resources, security policies, and data management [18]. In contrast, non-standalone networks leverage existing public 5G infrastructure for certain functions—such as coverage extension or traffic routing—while maintaining dedicated private resources [19]. Both approaches allow organizations to balance autonomy, performance, and cost-efficiency, depending on operational priorities [5].

Security is an integral aspect of private 5G network architecture. Advanced encryption protocols ensure data confidentiality and integrity, while robust authentication mechanisms safeguard against unauthorized access [8]. Network slicing allows the creation of multiple virtual networks within the same physical infrastructure, each with tailored security policies, resource allocations, and performance parameters, providing strong isolation for critical applications and specific user groups [20].

By integrating flexible infrastructure, embedded security, and versatile deployment options, private 5G networks establish a resilient and adaptive platform for mission-critical applications across industries. Figure 1 [9] illustrates the interconnection between RAN, core network, and UE, highlighting the essential components that support secure, high-performance communication.

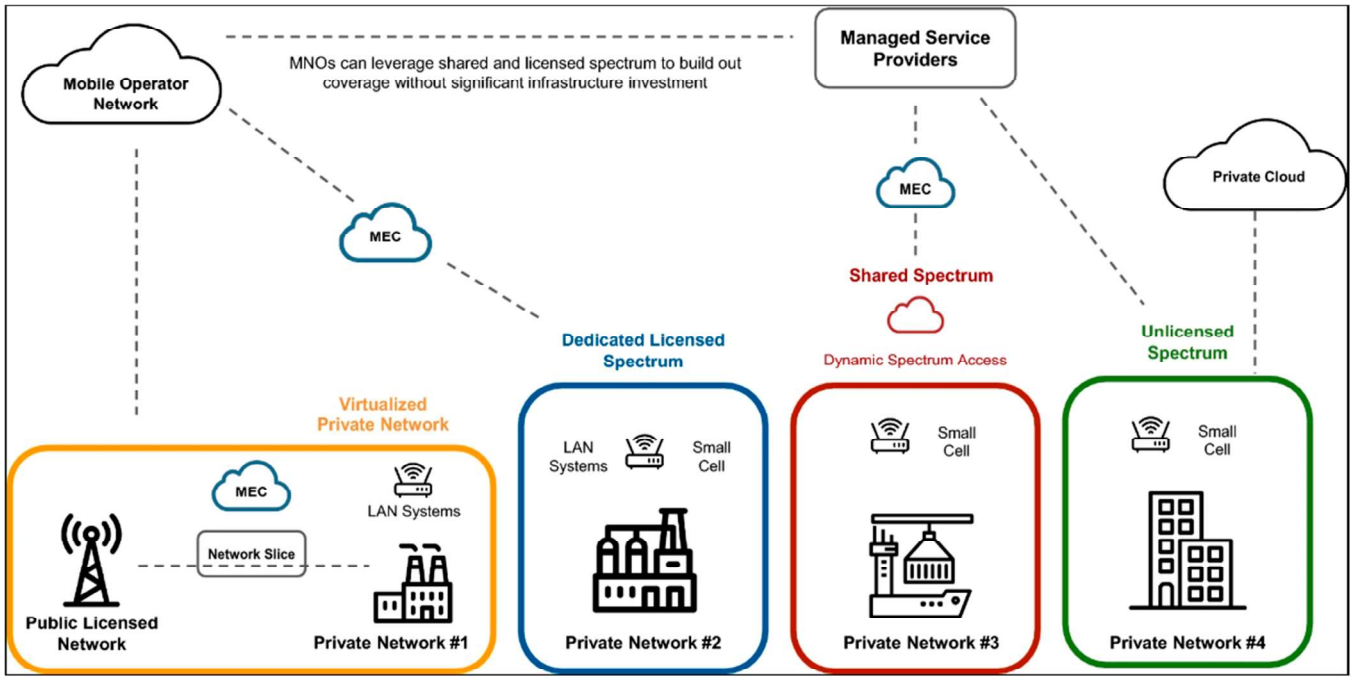

Figure 1. Architecture of Private 5G Networks. Note: This design was reprinted from "Private 5G networks: A survey on enabling technologies, deployment models, use cases and research directions by S. Eswaran and P. Honnavalli, Provided by the Springer Nature SharedIt content-sharing initiative. Copyright 2023 SpringerLink.

2.3. Security in 5G Networks

As 5G networks continue to expand across industries, they bring both unprecedented opportunities and significant security challenges. One key regulatory concern is the complexity and duration of spectrum allocation, which can delay deployment and expose networks to vulnerabilities [9,12]. Limited spectrum availability and rising costs particularly impact smaller organizations, potentially hindering equitable access to secure private 5G deployments [7,21].

Network slicing, a defining feature of 5G, enables multiple virtual networks to coexist on shared infrastructure. However, compromised slices may threaten other slices, placing sensitive data and mission-critical services at risk [8]. These vulnerabilities emphasize the importance of robust isolation mechanisms and continuous monitoring to maintain slice integrity.

Private 5G networks face threats to core security principles: authentication, confidentiality, integrity, availability, and non-repudiation [4]. The expanded attack surface exposes networks to Distributed Denial-of-Service (DDoS) attacks, eavesdropping, session

hijacking, spoofing, jamming, man-in-the-middle (MITM) attacks, and privacy breaches, particularly in critical sectors such as healthcare, industrial IoT, and smart cities [4,8,21]. To address these risks, attack graphs have proven effective in modeling potential attack paths, predicting vulnerabilities, and designing targeted defensive strategies [4,8].

Additional threats include traffic manipulation, malware injection, resource exhaustion, DNS cache poisoning, privilege escalation, and physical tampering with network components [22]. The scale and complexity of 5G networks magnify the consequences of these attacks, highlighting the necessity for proactive security measures. Recommended strategies include advanced encryption, multi-factor authentication, intrusion detection systems, and regular security audits to mitigate emerging and evolving risks [7,22].

Emerging network solutions—such as disaggregated software RAN, 5G Standalone (SA) Core, RAN sharing, and AI/ML-driven network optimization—offer enhanced performance but also introduce new vulnerabilities [11]. Moreover, the limited availability of certain security features primarily in Standalone networks can create a false sense of security, reinforcing the need for continuous validation and integration of security audits into operational frameworks [20].

In conclusion, securing private 5G networks requires a multi-layered and adaptive approach that addresses both traditional and emerging threats while maintaining operational performance, compliance, and resilience. Implementing such comprehensive strategies is essential to ensure that private 5G networks can reliably support mission-critical applications across diverse industrial and societal domains [7,11].

2.4. Summary of the Literature Review

This review carefully selected studies specifically addressing security vulnerabilities in private 5G networks, applying rigorous eligibility criteria to ensure both relevance and quality. The included articles encompass a wide spectrum of topics, ranging from emerging threat vectors and architectural weaknesses to proposed mitigation strategies, providing a comprehensive and structured overview of the security landscape in private 5G environments. By concentrating on high-quality research, the review captures not only current challenges but also critical areas requiring further investigation, supporting the design and implementation of robust security frameworks.

To reflect the most recent advancements and trends, the review prioritized publications from 2014 to 2024, ensuring that contemporary threats and novel security concerns in private 5G networks are adequately represented. Studies lacking empirical evidence, theoretical rigor, or direct relevance were excluded, guaranteeing that the findings are credible, academically rigorous, and practically meaningful. Furthermore, the selected literature integrates diverse methodologies and perspectives, enriching the synthesis and enabling a nuanced understanding of vulnerabilities, risks, and protective measures within private 5G deployments.

Overall, this curated body of work establishes a solid foundation for identifying knowledge gaps, informing effective mitigation strategies, and guiding future research directions, ultimately contributing to the development of secure, resilient, and trustworthy private 5G networks.

3. Methodology

This study applied a structured review methodology to analyze security vulnerabilities in private 5G networks. The approach ensured transparency, reproducibility, and an evidence-based synthesis of the most relevant academic and technical research.

3.1. Review Approach

The review served as the foundation for identifying, classifying, and synthesizing existing knowledge on 5G private network security. Its structured nature allowed for a transparent and replicable process, ensuring that findings are comprehensive and unbiased. The method included the formulation of guiding research questions, a multi-database search, critical appraisal of study quality, and thematic synthesis of the extracted data. This process was particularly suitable for an evolving research area such as private 5G security, where threats and mitigation techniques change rapidly.

3.1.1. Rationale for Using a Review

The choice of a review methodology was motivated by the complexity and dynamic nature of security vulnerabilities in private 5G environments. Prior research often emphasizes public 5G or general security models, leaving private implementations underexplored. A structured review allows researchers to systematically identify these research gaps and emerging vulnerabilities—especially in areas like network slicing, virtualization, and edge computing. This approach supports the identification of both well-established risks and less-documented attack vectors, ensuring a comprehensive understanding of current challenges and potential countermeasures.

3.1.2. Overview of the Review Process

The review was conducted through several key stages to ensure rigor and consistency. The process began with defining focused research questions, followed by the systematic search and selection of relevant studies. Each stage emphasized transparency and adherence to reproducible standards similar to PRISMA guidelines. After identifying eligible publications, data were extracted and organized into categories for comparative and thematic analysis. This sequence minimized bias and enhanced the reliability of conclusions while maintaining alignment with the research objectives.

3.2. Defining the Research Question

The review was guided by a central question:

What are the key security vulnerabilities in private 5G networks?

To refine this scope, three sub-questions were formulated:

1. What specific vulnerabilities exist within private 5G networks?
2. How do these vulnerabilities affect confidentiality, integrity, and availability?
3. What mitigation strategies have been proposed in the literature?

This structure ensured focus and completeness, directing the selection and analysis of studies toward the most relevant aspects of private 5G security.

3.3. Selecting Databases and Research Sources

To ensure academic quality and relevance, evidence from the literature was collected from leading databases: IEEE Xplore, ScienceDirect, SpringerLink, ResearchGate, and Google Scholar. These platforms were selected due to their strong coverage in telecommunications and cybersecurity. The time frame was set between 2014 and 2024, reflecting the main period of private 5G deployment and associated research. The inclusion of both peer-reviewed and grey literature (e.g., technical reports, white papers) allowed for a broader view of security challenges and ongoing industry solutions.

3.4. Defining Search Terms, Keywords, and Scope

A search strategy was designed around core concepts of 5G security and private networks. The primary keywords included:

"Private 5G Network," "Non-Public 5G Networks," "Standalone Non-Public Networks," "5G Network Security Challenges," and "Security Vulnerabilities in Private 5G Networks."

Boolean operators were used to refine searches and combine related terms. The defined scope focused exclusively on studies addressing security vulnerabilities, countermeasures, or risk assessment within private 5G environments. This ensured the inclusion of literature most relevant to confidentiality, integrity, and availability concerns.

3.5. Merging Results from Multiple Databases

Search results from the selected databases were merged into a unified dataset to eliminate duplicates and consolidate diverse perspectives. Combining sources such as IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar ensured balanced representation across both academic and technical domains. This process mitigated biases related to database indexing limitations and enabled the inclusion of interdisciplinary contributions, resulting in a robust foundation for thematic analysis.

3.6. Screening, Study Selection, and Eligibility Criteria

A multi-stage screening process ensured the inclusion of only high-quality and relevant studies.

Eligibility criteria included:

- Relevance: Studies addressing vulnerabilities, risks, or threats in private 5G networks.
- Recency: Publications between 2014 and 2024 to capture recent developments.
- Quality: Peer-reviewed sources or credible technical reports.

Exclusion criteria ruled out research focused solely on public 5G networks or unrelated technologies. After filtering an initial pool of over 300 studies, 55 articles were retained based on methodological rigor and thematic alignment. The process included initial title and abstract review, followed by full-text evaluation and final inclusion based on contribution quality.

3.7. Review and Data Extraction Process

Selected studies were analysed to extract key data regarding security domains, methodological approaches, and proposed solutions. Extracted elements included:

- Identified vulnerabilities such as jamming, spoofing, and edge-based threats.
- Proposed mitigation strategies including blockchain frameworks, quantum-safe cryptography, and zero-trust architectures.
- Implementation challenges like scalability and interoperability constraints.

Thematic analysis was applied to group findings into patterns and trends. This method facilitated the identification of both well-documented and emerging security concerns, as well as underexplored areas requiring future research attention.

3.8. Synthesizing the Results

The synthesis phase integrated insights across all selected studies to develop a consolidated view of private 5G security. Recurrent vulnerabilities—such as weak authentication, supply-chain exposure, and control-plane attacks—were frequently reported. At the same time, new research directions were identified, including AI-driven anomaly detection, adaptive encryption, and quantum-resistant solutions.

By mapping these findings, the review highlighted both consensus and divergence in the current literature, underscoring areas that remain insufficiently studied. The synthesis provides a foundation for understanding current limitations and guiding future work toward more resilient, adaptive security mechanisms in private 5G environments.

4. Results and Findings

The findings of this study stem from a comprehensive review of literature on security vulnerabilities in private 5G networks. The analysis highlights the evolving research landscape, exposing both critical vulnerabilities and the unique cybersecurity challenges inherent to private deployments. Unlike public 5G, private networks—customized to enterprise-specific requirements—introduce distinct risks shaped by their architecture, deployment models, and operational contexts.

While notable progress has been made in addressing general 5G security concerns, significant gaps remain in the design of frameworks tailored specifically for private deployments. Current approaches often overlook the bespoke configurations, localized infrastructures, and mission-critical applications that characterize these environments.

A comparative perspective further underscores the distinction between private and public 5G networks. Recognizing these differences is essential for developing targeted mitigation strategies capable of addressing the heightened risks of private 5G, particularly in sensitive domains such as industrial automation, healthcare, and smart cities.

4.1. Comparison of Security Vulnerabilities in Public and Private 5G Networks

Public and private 5G networks share a common architectural foundation but differ substantially in deployment contexts, operational models, and security challenges. The literature reveals overlapping vulnerabilities alongside risks unique to private deployments, underscoring the need for tailored protection strategies.

Authentication and Authorization Flaws. While both types of networks depend on authentication protocols, the consequences diverge. Public 5G relies on standardized 3GPP mechanisms but remains vulnerable to SIM jacking and identity spoofing [8]. Private 5G, by contrast, often suffers from weak access controls, insufficient role-based authentication, and limited use of multi-factor methods, exposing them to insider threats and unauthorized access in sensitive environments such as industrial automation and healthcare [4].

Data Privacy and Integrity Risks. Public networks face risks from large-scale traffic and cloud integration, which increase exposure to eavesdropping and tampering [8]. Private networks, though more contained, inherit vulnerabilities when interfacing with legacy systems or public infrastructure. Custom implementations may also introduce untested flaws, compounding risks [8].

Network Slicing Vulnerabilities. Slicing supports multiple virtual networks on shared infrastructure but is prone to cross-slice attacks when misconfigured [8,12]. In private networks, slices often segregate critical applications—such as healthcare or industrial IoT—where weak isolation or poor management can expose sensitive data and operations.

Denial-of-Service (DoS) Attacks. DoS affects both models but with different consequences. Public networks face large-scale disruptions to services like mobile internet and VoIP [21]. In private deployments, DoS attacks can halt mission-critical operations in sectors such as healthcare or manufacturing, resulting in severe financial and operational losses [13].

Systemic Challenges. Both network types of struggles with mitigation, yet private 5G is particularly affected by the lack of standardized frameworks [21]. The coexistence of IoT and legacy systems expands attack surfaces and often forces reliance on ad hoc security measures, unlike the more mature practices in public networks.

Conclusion. Although public and private 5G networks share common vulnerabilities, the bespoke configurations and operational demands of private deployments create unique challenges. Weak authentication, misconfigured slices, and legacy integration highlight the need for customized, sector-specific defenses. Table 2 summarizes the comparative vulnerabilities.

Table 2. Security Vulnerabilities and Challenges in Private 5G Networks: Impact Analysis.

Category	Vulnerability	Challenges	Impact
Spectrum and Authorization	Delays in spectrum allocation	Hinders timely network deployment	Slows innovation and market readiness
	Limited affordable spectrum	Barriers for small enterprises	Reduces competitiveness
	Lengthy authorization processes	Increases costs and delays	Reduces ROI and scalability.
Authentication and Access Control	Authentication issues	Risk of unauthorized access	Compromises security and user trust
	Weak access controls	Exploitation by attackers	Data breaches and disruptions
	Fake user equipment	Malicious device infiltration	Service disruptions and financial losses.
Confidentiality and Privacy	Inadequate data encryption	Privacy and data leaks	Financial and reputational damage
	Eavesdropping on communication	Interception of sensitive information	Regulatory penalties and data exposure
	Misconfigured security settings	Leaves exploitable gaps	Undermines reliability
Integrity and Availability	Service availability loss	Network disruptions	Affects business continuity
	Loss of data integrity	Corruption of critical data	Reduces trust and decision-making reliability
	Denial-of-Service attacks	Overloaded resources	Operational inefficiencies
	Signalling storms	Infrastructure overload	Network degradation or collapse.
Network Slicing and Orchestration	Slice isolation bypass	Risks to performance and data security	Compromised network integrity
	Orchestration challenges	Resource allocation inefficiencies	Reduces reliability.
Physical Security	Insider attacks	Risk of sabotage	Operational damage and data leaks
	Physical theft or vandalism	Loss of infrastructure	Downtime and repair costs
Specific Attack Types	Man-in-the-middle attacks	Data interception	Breaches and loss of trust
	Rogue base station attacks	Traffic manipulation	Data theft and service disruptions
	Device malware injection	Remote control of devices	Facilitates further attacks
	Jamming and channel interference	Disrupted communication	Affects service reliability
	DNS cache poisoning	Misdirected traffic	Phishing and service disruption
Machine Learning and AI	Vulnerable ML algorithms	Exploitation risks	Reduces optimization and reliability.
Radio Access Network (RAN) and Open Interfaces	Resource exhaustion	Overloaded resources	Reduces performance and quality
	Vulnerabilities in O-RAN	Increased security risks	Opens avenues for breaches

Table 2. *Cont.*

Category	Vulnerability	Challenges	Impact
Legacy Systems	Vulnerable legacy devices	Exploitation of outdated protocols	Reduces overall security.
	Difficulty with updates	Exposure to known vulnerabilities	Increases attack risks
Encryption and Cryptography	Weak cryptographic protection	Unauthorized data modification	Compromises data authenticity
	Insecure encryption key transmission	Risk of interception	Enables decryption of sensitive data
Specific Messaging Attacks	Exploitation of system messages	Network manipulation	Affects integrity and performance
	Fake base station attacks	Misguided user equipment	Data theft and service manipulation
Integration and Deployment	RAN sharing challenges	Complex infrastructure management	Affects efficiency and security
	Integration issues	Security gaps and deployment delays	Reduces reliability and scalability.
Expertise and Regulation	Limited 5G expertise	Improper configurations	Increased vulnerabilities
	Inconsistent regulations	Compliance gaps	Delays and security complications

Note. This data was collected from various literature used throughout the thesis, collected and put into this table. All authors have been cited.

4.2. Analysis of Findings

The literature review provided an in-depth examination of security vulnerabilities in private 5G networks, uncovering a wide spectrum of technical and operational challenges [11]. The studies emphasize that the highly customized architectures and diverse deployment scenarios of private 5G networks introduce risks distinct from those of public networks. Weaknesses in authentication and access control emerge as critical vulnerabilities, exposing sensitive operations to unauthorized access—an especially pressing concern in industrial and mission-critical applications [4].

4.2.1. Identified Security Vulnerabilities

Key threats include distributed denial-of-service (DDoS) attacks, which exploit 5G's scalability and low latency to disrupt operations, affecting sectors such as industrial automation, healthcare, and emergency services [1,5]. The proliferation of IoT devices further expands the attack surface, enabling large-scale botnet-driven attacks against the RAN, core network, or cloud-based services [6,21].

Spoofing attacks were found to compromise authentication processes and can serve as precursors to MITM or DoS attacks. They pose particular risks to industrial and healthcare systems [13,23]. While advanced 5G technologies such as massive MIMO and beamforming enhance performance, they may inadvertently create new spoofing vectors [4,13].

Unauthorized access remains a major concern due to weak authentication protocols, insufficient access controls, and supply chain vulnerabilities [1,22]. Compromised hardware or software can grant attackers persistent network access, highlighting the importance of rigorous vendor vetting and cryptographic validation of updates [23].

Jamming attacks severely undermine service reliability in critical domains such as smart healthcare [13,21]. Botnet-driven coordinated jamming further magnifies disruptions.

Man-in-the-Middle (MITM) attacks jeopardize confidentiality, integrity, and availability [20,21,24].

Eavesdropping is often enabled by insecure protocols or physical proximity to victim devices [13,25,26]. These attacks can result in identity theft, financial loss, and reputational harm.

Weak passwords, biometric vulnerabilities, and poorly implemented multi-factor authentication (MFA) expose networks to credential-stuffing and unauthorized access [4,22,27,28].

Rogue base stations (FBS) and fake user equipment (UE) exploit authentication flaws to intercept communications, manipulate resources, and compromise network slices. These attacks endanger privacy, service continuity, and operational integrity [4,6,8,13,24,25,27].

The absence of standardized security frameworks for private 5G networks results in inconsistent implementations and elevated risk [7,24]. Collaborative efforts among technology providers, operators, and regulators are essential to establish best practices, exchange threat intelligence, and strengthen resilience [4,5,21].

Contextual Insights. Research gaps persist in the comparative analysis of private 5G networks with legacy systems, as well as in applying advanced threat modeling techniques—such as attack graphs—to this context [8]. Addressing these gaps is crucial to developing resilient frameworks that can mitigate evolving threats.

Overall, the findings reveal a complex threat landscape for private 5G networks, encompassing authentication weaknesses, encryption flaws, DDoS and spoofing risks, and regulatory challenges. Effective mitigation will require targeted research, robust security frameworks, and coordinated stakeholder collaboration to ensure secure deployment across critical sectors.

4.2.2. Themes and Patterns

The synthesis of the reviewed literature reveals several key themes and patterns that highlight both the challenges and opportunities associated with private 5G networks.

Regulatory and Deployment Challenges: A prominent theme concerns the regulatory and deployment hurdles faced by organizations adopting private 5G networks. Extended spectrum allocation timelines can delay network implementation and hinder technological advancement [12,29]. Limited availability of affordable spectrum further constrains deployment, particularly for smaller enterprises, while the complexity and cost of authorization processes impose additional financial and logistical burdens [9,12]. These findings underscore the need for streamlined regulatory frameworks and accessible spectrum allocation to enable efficient and secure adoption of private 5G technologies.

Authentication and Access Control: Robust authentication mechanisms are critical for safeguarding private 5G networks [13]. Weak access controls can compromise data confidentiality and integrity, while non-repudiation mechanisms are essential to trace actions to specific users. Software-Defined Perimeter (SDP) technologies establish secure perimeters around sensitive resources, applying a zero-trust model that grants access based on identity rather than location [17]. Complementary measures, including multi-factor authentication (MFA) and device authentication protocols, further enhance resilience against unauthorized access [26].

Network Slicing and Isolation Risks: Network slicing allows for the partitioning of resources to support diverse applications, but it introduces vulnerabilities in private 5G networks [22,30]. Inadequate slice isolation can result in cross-slice contamination, traffic manipulation, data leakage, or denial-of-service attacks. Attackers may exploit slicing weaknesses to intercept or redirect traffic, undermining both service quality and security. Effective mitigation strategies require advanced encryption, strict authentication, secure slicing mechanisms, AI-driven monitoring, anomaly detection, and intrusion prevention systems [22,30].

Diverse Attack Vectors: Private 5G networks face a wide spectrum of threats, including fake base stations (spoofing), Denial-of-Service (DoS), eavesdropping, tampering, and IMSI-catching [23,24,31]. Spoofing and rogue base stations allow attackers to intercept communications or manipulate network traffic, while DoS attacks can disrupt critical services. Tampering compromises data integrity, and passive threats, such as IMSI leaks, expose users to tracking and targeted attacks. These vulnerabilities emphasize the necessity of a multi-layered security approach, incorporating adaptive authentication, strong encryption, intrusion detection, and continuous monitoring to protect private 5G networks against evolving cyber threats [24].

Similarities

Common Threats: Across the reviewed studies, several critical security threats consistently affect private 5G networks. Distributed Denial-of-Service (DDoS) attacks are highlighted as a primary concern due to their potential to overwhelm network resources and disrupt essential services [13,22,24]. Spoofing attacks, particularly via fake base stations, enable interception of communications, data theft, or traffic manipulation [23,31]. Weak authentication and access control frameworks further exacerbate risks, leaving networks vulnerable to unauthorized access in environments with multiple devices and users [13,17].

Eavesdropping and data tampering remain significant risks when encryption protocols are inadequate [23]. Network slicing vulnerabilities, including slice isolation bypass and traffic manipulation, threaten data integrity and service continuity [22,31]. Radio-layer threats, such as jamming and IMSI leaks, compromise network performance and user privacy [13,24]. Collectively, these shared vulnerabilities highlight the multifaceted threats facing private 5G networks and underscore the need for coordinated, multi-layered security strategies.

Need for Improved Security Measures: Multiple studies emphasize the urgency of tailored security solutions for private 5G deployments [13,24]. Traditional authentication mechanisms are often insufficient for critical applications such as industrial IoT and smart healthcare. Proposed solutions include Software-Defined Perimeter (SDP) frameworks, enforcing strict trust-based authentication to mitigate unauthorized access [17,32]. Complementary measures, including multi-factor and device authentication protocols, further strengthen defenses [26].

The literature also highlights the need for standardized security frameworks, as current models inherited from public 5G or legacy systems fail to address private network challenges. Key gaps include:

- Network slicing security: Ensuring complete isolation between slices.
- Zero-trust architectures: Continuous verification for all users and devices [23].
- Advanced cryptography: Implementing quantum-resistant encryption.

Collaboration among network operators, device manufacturers, and regulators is critical to establish best practices, share threat intelligence, and enhance overall network resilience.

Differences

Proposed Solutions: Studies present diverse approaches to mitigating private 5G vulnerabilities, reflecting the layered complexity of these networks. Reference [17] propose an SDP framework to enforce strict authentication and isolate network resources, addressing systemic weaknesses. In contrast, [31] focuses on specific threats, such as fake base stations, advocating for real-time detection algorithms and monitoring tools.

Other proposed approaches include:

- AI-based threat detection: Real-time anomaly identification [4].
- Blockchain security: Enhancing trust and data integrity via distributed ledgers [33].

- Zero-Trust Network Access (ZTNA): Continuous verification beyond perimeter defenses [32].

These variations highlight the necessity of adaptive, multi-layered strategies that combine architectural innovations with targeted countermeasures.

Focus Areas: Studies also differ in scope. Sector-specific analyses, such as private 5G in smart healthcare, emphasize tailored security solutions to address authentication, confidentiality, and non-repudiation issues [13,22]. Broader cross-industry studies examine common vulnerabilities, including network slicing risks, DoS, spoofing, and eavesdropping, providing a holistic perspective relevant to multiple applications [23,31,34].

This contrast between targeted and generalized analyses underscores the need for flexible frameworks that balance specificity with broad protection. Table 3 summarizes the key vulnerabilities identified, offering stakeholders a structured reference to prioritize mitigation strategies and strengthen private 5G security.

Table 3. Common security Threats associated in Private 5G Networks.

Category	Security Vulnerability	Description
Network Attacks	Distributed Denial-of-Service (DDoS) Attacks	Overwhelm network resources, disrupting critical services by exploiting increased connectivity and bandwidth.
Identity and Authentication Threats	Spoofing Attacks	Attackers impersonate legitimate network entities; fake base stations can intercept communications, steal data, or manipulate network traffic.
	Authentication and Access Control Vulnerabilities	Weak authentication frameworks make networks susceptible to breaches; secure and scalable authentication is required.
Data Security Risks	Eavesdropping and Data Tampering	Weak encryption protocols allow attackers to intercept sensitive data or alter transmissions, compromising network integrity.
Network Slicing Threats	Slice Isolation Bypass and Traffic Manipulation	Attackers exploit vulnerabilities in one slice to affect others, undermining overall network security.
Radio-Layer Vulnerabilities	Active Threats: Radio Jamming and Signal Overshadowing	Degrade network performance by interfering with wireless signals.
	Passive Threats: IMSI Leaks	Compromise user privacy by exposing unique subscriber identifiers.

The findings from the literature review reveal a comprehensive spectrum of security vulnerabilities and challenges unique to private 5G networks. Across the reviewed studies, several recurring themes consistently emphasize the complexity of securing these networks against evolving threats:

1. Regulatory and Deployment Challenges: Private 5G deployment is often constrained by regulatory barriers, including prolonged spectrum allocation processes and limited access to affordable spectrum. These obstacles create logistical and financial burdens, hindering widespread adoption. Streamlined regulatory frameworks and improved spectrum accessibility are essential to enable timely and secure deployment of private 5G technologies.
2. Authentication and Access Control: Robust authentication mechanisms are crucial for protecting private 5G networks. Vulnerabilities in existing systems—particularly those managing sensitive or mission-critical data—pose significant security risks. Proposed solutions, such as Software-Defined Perimeter (SDP) architectures, enforce secure, identity-based access and strengthen overall network resilience.

3. Network Slicing and Isolation Risks: Network slicing offers essential benefits for resource allocation and traffic management; however, inadequate isolation between slices can introduce severe security risks, including cross-slice contamination and unauthorized data manipulation. Effective mitigation requires advanced encryption, strict isolation protocols, and continuous monitoring to ensure slice integrity and safeguard sensitive resources.
4. Diverse Attack Vectors: Private 5G networks face a broad array of threats, including spoofing, fake base station attacks, denial-of-service (DoS) attacks, and eavesdropping. These vulnerabilities jeopardize the confidentiality, integrity, and availability of data. The diversity and complexity of these attack vectors highlight the need for adaptive, multi-layered security strategies capable of addressing both known and emerging threats.
5. Proposed Solutions: The literature presents multiple mitigation approaches, ranging from comprehensive architectural frameworks, such as SDP, to targeted interventions like real-time detection algorithms for fake base stations. Additional strategies include enhanced authentication frameworks, zero-trust architectures, and sector-specific countermeasures. The variety of proposed solutions underscores the importance of integrated, layered security measures customized to the operational context of private 5G deployments.
6. Sector-Specific Security Concerns: Certain sectors, such as smart healthcare, exhibit unique security requirements where data confidentiality and real-time communication are critical. While some studies advocate generalizable security frameworks, the evidence emphasizes the need for solutions tailored to sector-specific operational and regulatory constraints.

Overall, the findings illustrate the intricate nature of securing private 5G networks. They highlight the necessity of adaptive, collaborative, and context-aware strategies that integrate advanced security technologies, regulatory improvements, and industry-specific considerations. Table 4 presents recommended security best practices, providing a structured reference for mitigating vulnerabilities and maintaining robust protection in private 5G networks.

Table 4. Security Best Practices for Private 5G Networks.

Security Best Practice	Description	Implementation Considerations	Effectiveness
Zero Trust Architecture (ZTA)	Requires strict identity verification for every user and device accessing the network.	Involves continuous authentication and least-privilege access controls.	Highly effective in preventing unauthorized access.
Network Slicing Security Protocols	Implements isolation and strict security policies for each network slice.	Requires careful resource allocation and segmentation.	Prevents cross-slice attacks and lateral movement of threats.
End-to-End Encryption (E2EE)	Encrypts data throughout transmission to prevent unauthorized interception.	Requires strong key management policies.	Essential for maintaining confidentiality and data integrity.
Multi-Factor Authentication (MFA)	Uses multiple verification factors to authenticate users and devices.	May impact usability and require additional infrastructure.	Strengthens access control and reduces credential theft risks.
Intrusion Detection and Prevention Systems (IDPS)	Monitors network traffic for anomalies and mitigate potential threats.	Needs proper tuning to reduce false positives.	Crucial for identifying and blocking security breaches.

Table 4. *Cont.*

Security Best Practice	Description	Implementation Considerations	Effectiveness
Access Control Policies	Defines and enforces restrictions on who can access network resources.	Requires continuous policy updates and role-based access control (RBAC).	Helps mitigate insider threats and unauthorized access.
Physical Security Measures	Protects network infrastructure from theft, tampering, or sabotage.	Includes secure facility access and monitoring.	Essential for preventing hardware-based attack.
Security in Third-Party Integrations	Ensures security compliance for external vendors and service providers.	Requires continuous assessment of third-party risk exposure.	Reduces vulnerabilities introduced by external components.

5. Security Challenges in Private 5G Networks

Private 5G networks, while delivering notable advantages in performance, reliability, and control, also introduce distinctive security challenges that must be addressed to ensure safe and resilient operation. These risks arise from the inherent characteristics of 5G technology, the specific demands of private deployments, and the rapidly evolving cyber threat landscape. As adoption expands across industries, the mitigation of these vulnerabilities becomes increasingly critical.

A central concern is the expanded attack surface. Deployments in manufacturing, ports, and smart cities often involve vast numbers of IoT devices and endpoints [4]. Each device represents a potential entry point, and their heterogeneity—ranging from basic sensors to autonomous systems—complicates the enforcement of consistent security policies. Compromised endpoints can provide attackers with unauthorized access, enable data breaches, or disrupt critical operations [15].

Network slicing security presents additional challenges. While slicing enables the creation of virtualized networks tailored to specific applications such as industrial automation or IoT, improper isolation can expose slices to cross-slice attacks, undermining system integrity [8]. Key risks include inter-slice resource exploitation, lateral movement of threats, and insufficient enforcement of slice-specific security policies.

The integration of edge computing further complicates security. Although edge computing reduces latency and enhances performance, distributed edge nodes often lack the robust protections of centralized data centers, leaving them exposed to both physical and cyberattacks [8]. Ensuring secure data transmission between edge and core infrastructures is essential [1], while AI-driven anomaly detection mechanisms are increasingly proposed to support real-time monitoring and rapid incident response [17].

The coexistence of legacy systems with private 5G infrastructures introduces another layer of risk. Many IT and OT legacy systems lack modern encryption, authentication, and patching capabilities, creating exploitable weaknesses [8]. Mitigating these risks requires compatibility controls, network segmentation, and continuous vulnerability assessments.

Insider threats remain a persistent challenge. Weak credential management and inadequate monitoring heighten risks from employees, contractors, or third parties [23]. Effective countermeasures include multi-factor authentication (MFA), role-based access control (RBAC), behavioral analytics, and comprehensive security awareness training.

The broader cyber threat landscape amplifies these challenges. With their high speed and low latency, private 5G networks are attractive targets for advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and ransomware campaigns [13]. Defenses must therefore include proactive measures such as real-time threat intelligence, automated orchestration, anomaly detection, and continuous patching.

Monitoring and incident response are particularly difficult in distributed 5G environments. Traditional solutions often fail to address the scale and complexity of private 5G and industrial IoT deployments [22]. Enhanced visibility requires zero-trust architectures, Security Information and Event Management (SIEM) platforms, and automation to support forensic analysis and rapid response.

In summary, securing private 5G networks requires a multidimensional strategy that integrates technical, operational, and human-centric measures. Strong encryption, secure authentication, network segmentation, continuous monitoring, and proactive threat intelligence form the foundation of resilience. As adoption accelerates, the ability of organizations to adapt and deploy layered defenses will be crucial to maintaining robust protection. Table 5 provides a high-level overview of these security challenges.

Table 5. High -Level Security Concerns in Private 5G Networks.

Category	Key Concerns
Expanded Attack Surface	The high number of connected devices and IoT endpoints increases potential entry points for cyber threats.
Network Slicing Complexity	Ensuring effective slice isolation, managing inter-slice communication security, and preventing unauthorized access to network slices.
Edge Computing Security	Protecting edge nodes from physical tampering, cyber threats, and data breaches while ensuring secure processing and transmission.
Integrating Legacy Systems	Older infrastructure may lack modern encryption, have unpatched vulnerabilities, and be incompatible with secure authentication protocols.
Insider Threats	Employees or contractors with legitimate access could unintentionally or intentionally compromise security.
Evolving Threat Landscape	Defending against advanced persistent threats (APTs), ransomware, and large-scale DDoS attacks targeting 5G networks
Security Monitoring and Response	The challenge of real-time threat detection, automated response, and forensic analysis in a highly distributed private 5G environment.
Authentication and Access Control	Enforcing robust identity verification for users, devices, and services to prevent unauthorized access
Regulatory and Compliance Risks	Ensuring compliance with GDPR, PCI DSS, and industry-specific security regulations, which may introduce additional constraints.
Data Confidentiality and Integrity	Protecting sensitive data in transit and at rest from unauthorized access, modification, or leakage, particularly in mission-critical applications
Regulatory and Compliance Challenges	Dependencies on vendors, cloud providers, and third-party software/hardware components introduce supply chain vulnerabilities.
Third-Party Security Risks	Safeguarding physical network components such as base stations, edge nodes, and core network infrastructure from tampering, destruction, or theft
Physical Security	Protecting base stations, network infrastructure, and edge devices from tampering, destruction, or unauthorized access.

5.1. Threats to Data and Services in Private 5G Networks

5.1.1. Risks to Confidentiality, Integrity, and Availability of Data

Eavesdropping and Privacy Leaks: Eavesdropping represents a major threat to the confidentiality, integrity, and availability (CIA) of data in private 5G networks [35]. By intercepting communications, attackers can obtain sensitive information such as personal records, corporate secrets, or financial transactions [13]. This not only compromises con-

fidentiality but also enables the manipulation of intercepted data, undermining integrity. For instance, altered medical records or financial transactions can cause severe harm.

The consequences extend beyond technical disruption. Individuals may face identity theft and financial loss [4], while organizations risk corporate espionage, intellectual property theft, and reputational damage. Availability can also be indirectly impacted, as attackers leverage stolen data to launch denial-of-service (DoS) attacks. Privacy leaks, often enabled by weak encryption, misconfigured access controls, or poor data handling, further exacerbate these risks [15]. Given the large volumes of sensitive data in healthcare, finance, and manufacturing, even minor lapses can result in significant breaches [35].

Why it is critical for data sectors such as healthcare, finance, and manufacturing depend heavily on data protection for continuity, compliance, and customer trust [27]. Eavesdropping directly violates confidentiality regulations such as HIPAA, GDPR, and CCPA [13], exposing organizations to legal, financial, and reputational repercussions. Moreover, tampering with intercepted data undermines integrity, while availability may be compromised by secondary DoS attacks. Because these intrusions often remain undetected for extended periods [27], strong encryption, strict access control, and proactive monitoring are indispensable safeguards.

Spoofing attacks using fake user equipment (UE) exploit weaknesses in device authentication, enabling unauthorized access to data and services [8]. Impersonating legitimate devices allows attackers to compromise confidentiality by accessing sensitive data [23], jeopardize integrity by injecting falsified information, and degrade availability by overloading resources or initiating DoS attacks [24].

The risks span multiple sectors. In healthcare, spoofing can expose patient records; in finance, it may reveal transactions and facilitate fraud [4]; and in industrial environments, falsified sensor data can disrupt operations. These attacks are difficult to detect and may persist over long periods. Addressing them requires advanced authentication mechanisms, real-time threat monitoring, and collaboration between operators, equipment vendors, and security experts [8].

Data integrity is a particular concern for private 5G networks as spoofed devices can introduce manipulated data into critical systems [25]. In manufacturing, this could cause unsafe machine configurations [5], while in smart cities, falsified data could disrupt traffic or energy grids [9]. Such covert manipulations undermine trust in decision-making processes. Robust authentication, continuous validation of data integrity, and advanced monitoring are therefore essential [6].

Authentication forms the foundation of private 5G network security [13]. Weak or inconsistent implementations—particularly among diverse IoT and industrial devices—create vulnerabilities that attackers exploit to bypass controls and gain unauthorized access [25]. Once inside, attackers can escalate privileges, manipulate configurations, disable protections, and disrupt services. Devices with outdated firmware or limited computational capacity are especially vulnerable.

Data authentication is the first barrier against unauthorized access [22], and weak mechanisms compromise confidentiality through data theft, undermining integrity by enabling data manipulation, and threatening availability by facilitating DoS attacks [1]. To mitigate these risks, strong multi-factor authentication (MFA), role-based access control (RBAC), and real-time monitoring are vital. Without these measures, private 5G networks remain exposed to advanced persistent threats with severe implications [22].

5.1.2. Risks of Confidentiality, Integrity, and Availability of Services

Distributed Denial-of-Service (DDoS) Attacks are a critical threat to service availability in private 5G environments. The impact of this kind of attacks is magnified in mission-

critical sectors that rely on private 5G, including healthcare, manufacturing, and smart cities. In healthcare, disruptions to real-time monitoring or remote surgery can delay treatment and pose life-threatening risks [13]. In manufacturing, halted production lines cause financial losses and equipment damage [21], while in smart cities, attacks on traffic or public safety systems can trigger cascading failures [15].

Beyond availability, DDoS attacks often serve as smokescreens for intrusions aimed at data theft, thereby undermining confidentiality and integrity [36]. The scalability and low latency of private 5G exacerbate these risks, expanding the attack surface. Without measures such as filtering, rate limiting, and anomaly detection, attackers can exploit these characteristics to amplify assaults [13]. Strengthening resilience against DDoS attacks is therefore essential for ensuring continuous, reliable services.

Disrupted communications caused by jamming attacks in industrial systems can halt production [37], while in healthcare, interruptions in telemedicine or monitoring can endanger patients [13]. Similarly, smart city services like traffic control or emergency communications are highly vulnerable [38].

The susceptibility of 5G to jamming is heightened by its reliance on millimetre-wave frequencies, which are prone to attenuation and interference [1]. The dense device environments characteristic of private 5G exacerbate disruptions, as a single attack may ripple across interconnected systems [7]. Mitigation requires countermeasures such as frequency hopping, directional antennas, and interference detection to maintain service reliability and prevent cascading failures [5].

With Man-in-the-Middle (MITM) Attacks hackers may steal credentials [27], exploit financial transactions [13], or manipulate control commands. In industrial automation, altered signals can lead to unsafe machine operations or production defects [22], while in healthcare, tampered patient data can result in misdiagnosis or delayed treatment [13].

Service availability is also at risk: disruptions in synchronization for autonomous vehicles can cause accidents, while false commands in energy grids may trigger cascading failures [2]. MITM attacks often exploit weaknesses in protocols and authentication via DNS spoofing, hijacking, or rogue access points. Countermeasures such as end-to-end encryption, mutual authentication, and intrusion detection systems [1] are essential to maintain the reliability of mission-critical services.

Fake Base Station (Fake BS) Attacks may intercept communications, compromise confidentiality, and disrupt availability. IMSI-catching exposes user identities [13], while the manipulation of unicast or paging messages enables injection of false commands, causing service mismanagement in domains such as healthcare and industrial automation. Redirecting UEs away from real base stations can also deny access to essential services, a critical risk in emergency response or industrial contexts [24]. These attacks are further complicated by multi-stakeholder environments involving CSPs and VMNOs, where differing priorities can hinder uniform protections [6]. The reliance on cloud-based storage across jurisdictions additionally raises privacy concerns. Effective mitigation requires fake BS detection mechanisms, stricter access controls, and coordinated security frameworks among stakeholders to ensure the confidentiality, integrity, and availability of services.

5.2. Use Case

Securing private 5G networks requires addressing complex challenges, particularly in the domain of network slicing. A major concern is slicing isolation bypass, which allows attackers to move laterally between slices, breaching logical boundaries and gaining unauthorized access to sensitive data or services [22]. Since network slicing is a foundational 5G feature that enables multiple virtual networks to coexist on shared infrastructure, fail-

ures in isolation mechanisms can result in severe breaches, particularly in mission-critical environments such as industrial automation, healthcare, and smart grids.

Network slicing depends on Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for dynamic resource allocation [39]. While these technologies enhance flexibility, misconfigurations or vulnerabilities in slice management may enable attackers to gain unauthorized access, manipulate control commands, or launch Denial-of-Service (DoS) attacks. Such incidents could cause data leakage, service disruption, or even loss of control over critical infrastructure.

Regulatory and operational constraints further complicate security. Variations in national regulations and spectrum licensing create inconsistencies in protection mechanisms, broadening the attack surface across jurisdictions [12]. Local 5G operators—particularly those outside traditional telecom ecosystems—often lack sufficient expertise or mature security frameworks to ensure resilience. Moreover, lengthy authorization processes for radio equipment can delay critical updates, leaving networks exposed to emerging threats. The need to comply with sector-specific and cross-border data protection requirements adds another layer of complexity, particularly in industrial or governmental contexts where sensitive data is exchanged [12].

A practical illustration of these risks is found in Vehicle-for-Hire (VFH) applications. Dedicated slices provide ultra-reliable, low-latency communication for fleet management, navigation, and customer interaction. However, attackers may exploit vulnerabilities in slice isolation or handover (HO) mechanisms to disrupt services or mount location-based attacks. Route deviations can interfere with HO processes, making networks susceptible to jamming, rogue base stations, or unauthorized interception. These weaknesses may expose real-time location data, degrade service quality, and compromise user trust [40].

The integration of contextual factors—such as traffic patterns, institutional rules, and human behavior—adds additional uncertainties that adversaries may exploit. For instance, simulation frameworks like the Ingolstadt Traffic Scenario for SUMO (InTAS), which align real-time traffic dynamics with slice resource allocation, could be targeted to manipulate simulations, disrupt fleet coordination, or compromise both physical and digital infrastructures [40].

Mitigation strategies must include robust slice isolation mechanisms, AI-driven anomaly detection, and advanced intrusion detection systems [8]. Additionally, regulatory harmonization is essential to establish consistent protection measures across jurisdictions. Together, these safeguards are critical for ensuring the confidentiality, integrity, and availability (CIA) of services, thereby securing mission-critical applications within private 5G networks [1].

6. Mitigations

Private 5G networks, increasingly deployed in mission-critical environments such as healthcare, industry, and smart grids, demand adaptive mitigation strategies to preserve confidentiality, integrity, and availability (CIA). The literature identifies a range of defensive mechanisms—encryption, IDS/IPS, and authentication protocols—supplemented by emerging techniques such as quantum-resistant cryptography, machine learning-based anomaly detection, and multi-factor authentication (MFA) [1,4,7,8,13,21–24,26,33,41–47]. These measures must be adapted to heterogeneous devices, network slicing, and edge-virtualized environments, where scalability and latency constraints often limit their efficiency. The multi-stakeholder character of private 5G ecosystems—spanning CSPs, VMNOs, and cloud providers—further complicates accountability and enforcement.

Jamming Attacks.

Countermeasures include spread-spectrum and frequency-hopping techniques, encrypted control channels, redundancy, and adaptive power control [21,23,41]. IDS/IPS support real-time detection and automated reaction to interference [4,24]. Regular updates of software and hardware reduce exposure to known vulnerabilities [1]. Together, these mechanisms provide layered protection to maintain service continuity in critical infrastructures.

Man-in-the-Middle (MITM) Attacks.

Segmentation, isolation, and strict access control prevent interception [22,42], while end-to-end encryption (TLS, IPSec) and MFA mitigate credential misuse [4]. Incident-response planning and blockchain-based key verification reinforce trust [4,26]. Mutual authentication and machine learning-driven anomaly detection further enhance defence against evolving MITM threats [1,21].

Denial-of-Service (DoS) Attacks.

DoS/DDoS attacks exploit vulnerabilities in slicing and control planes [7,13]. Mitigation relies on layered defences combining IDS/IPS, traffic filtering, DNS protection, anti-DDoS appliances, and redundant network paths [21]. Adaptive traffic management and edge-based anomaly detection safeguard resources and ensure operational continuity [13].

Spoofing Attacks.

Robust mutual authentication, PKI-based certificates, and CSI-based physical-layer verification help prevent impersonation [4]. Machine-learning anomaly detection assists in identifying spoofing attempts, complemented by continuous patching and collaborative refinement of protection mechanisms.

Fake User Equipment (UE).

Mitigation integrates 5G AKA, edge-based security, and supply-chain validation to block malicious devices [7,8,43]. Network isolation and awareness training reduce exposure to social-engineering vectors [22].

Fake Base Stations (FBS).

Digital-signature-based authentication of system messages and PKI solutions under development by 3GPP provide preventive assurance [4,44]. Reactive monitoring of UE behaviour, network-side analytics, and MFA-protected cryptographic keys increase overall resilience [21,24,45].

Authentication Issues.

Advanced mechanisms such as AKA and EAP support mutual verification in standalone deployments [13], while VPN SSC and MFA secure remote access [8]. Dynamic policies managed by AGUPF and AGPA enable adaptive responses [13]. Secure key management and logging strengthen RRC and UP integrity [46].

Unauthorized Access.

Controls such as MFA, RBAC, and least-privilege enforcement mitigate internal threats [4]. Segmentation restricts lateral movement, and physical safeguards protect infrastructure. Regular audits and continuous monitoring improve resilience [22].

Eavesdropping and Privacy Leaks.

Strong encryption (AES, E2EE), network segmentation, and strict access control reduce exposure [21,47]. Continuous monitoring via IDS/IPS and log analysis enhances detection [8]. Physical protection and MFA-based access further safeguard confidentiality [22,33]. In Table 6, we show a Summary of Attacks and Mitigation Strategies and the references in Private 5G Networks.

Table 6. Summary of Attacks and Mitigation Strategies in Private 5G Networks.

Attack Type	Key Mitigation Strategies	References
Jamming	Spread Spectrum Techniques (SST); frequency hopping; random key distribution; control channel protection; redundancy mechanisms; power control; IDPS detection and response; regular updates.	[1,4,21,23,24,41]
Man-in-the-Middle (MITM)	Network isolation and segmentation; end-to-end encryption (TLS, IPSec); MFA; advanced IDPS; incident response planning; user awareness; blockchain-based key verification; mutual authentication; anomaly detection with ML.	[1,4,21,22,26,42]
Denial of Service (DoS/DDoS)	Real-time detection via IDPS; traffic filtering and rate limiting; DNS protection; anti-DDoS appliances; redundant infrastructure; adaptive traffic management; edge anomaly detection; cloud security for slicing and RAN.	[7,13,21]
Spoofing	Mutual authentication; PKI and certificates; CSI-based authentication; ML-based anomaly detection; regular software/firmware updates; multi-stakeholder collaboration.	[4]
Fake User Equipment (UE)	5G AKA authentication; edge-based detection; supply chain validation; network isolation; user awareness training to prevent phishing/social engineering.	[7,8,22,43]
Fake Base Stations (FBS)	Digital signature-based authentication of system info; PKI-based approaches (3GPP); UE behaviour analysis (registration patterns); enhanced monitoring/logging; MFA or cryptographic keys at UE side.	[4,21,24,44,45]
Authentication Issues	Advanced protocols (AKA, EAP); VPN SSC with MFA; dynamic authentication (AGUPF, AGPA); secure key management between MeNB–SgNB; access logging and monitoring.	[8,13,46]
Unauthorized Access	MFA, RBAC, least privilege enforcement; network segmentation; physical security of infrastructure; user training and awareness; continuous audits and monitoring.	[4,22]
Eavesdropping & Privacy Leaks	Strong encryption (AES, E2EE); network segmentation; strict access control; IDS/IPS monitoring; log analysis; physical security; MFA and digital certificates.	[8,21,22,33,47]

7. Discussion and Future Directions

This review examined security vulnerabilities in private 5G networks, synthesizing insights from both academic and industry research to map current threats, challenges, and risks. The review pursued two primary objectives: (i) to identify and categorize the most critical vulnerabilities affecting confidentiality, integrity, and availability (CIA); and (ii) to assess their practical implications for network administrators, service providers, regulators, and end-users. By bridging academic findings with real-world applications, the study offers actionable recommendations for strengthening the security posture of private 5G environments.

The review uncovers a wide spectrum of vulnerabilities, including weaknesses in authentication and access control, risks from network slicing, exposure to Distributed Denial-of-Service (DDoS) attacks, and advanced threats such as rogue base stations and signal overshadowing. Additional concerns involve insufficient encryption, insider threats, and orchestration or virtualization flaws. Collectively, these findings emphasize the urgent need for adaptable, multi-layered security frameworks specifically designed for private 5G architectures.

The practical implications extend across stakeholders. For network administrators, the identification of common attack vectors provides a roadmap for prioritizing defenses. Service providers can reinforce compliance with standards and regulations, while policy-

makers may leverage these insights to guide spectrum allocation, authorization procedures, and security standardization. Nevertheless, significant research gaps remain. Empirical evidence regarding the long-term effectiveness of mitigation strategies is limited, particularly in dynamic and evolving threat landscapes. While promising solutions—such as Software-Defined Perimeter (SDP) architectures and moving target defence—have been proposed, real-world validation within private 5G networks is still sparse. Furthermore, domain-specific contexts, such as smart healthcare and industrial IoT, require deeper investigation into their unique security requirements.

A detailed analysis of the literature confirms recurring patterns of concern. DDoS attacks are particularly alarming due to their potential to disrupt mission-critical applications. Spoofing and unauthorized access, exacerbated by high device density, undermine network integrity. Jamming and man-in-the-middle (MITM) attacks expose vulnerabilities in communication channels, while eavesdropping and privacy leaks threaten user confidentiality, especially in sensitive sectors. Tampering with devices or data, along with fake base station attacks, highlights the sophistication of adversaries and underscores the necessity of robust, layered security measures.

Addressing these threats demands advanced authentication, stronger encryption protocols, continuous monitoring, and adaptive intrusion detection. Future research should prioritize real-world evaluation of proposed countermeasures, development of cross-domain security frameworks, and harmonization of regulatory standards. Collaboration among academia, industry, and regulatory bodies is essential to anticipate emerging threats and to build resilient private 5G systems capable of supporting critical applications with trust, reliability, and security.

7.1. Implications and Future Research Directions

7.1.1. Implications for Practice

This review highlights critical implications for securing private 5G networks, given their unique vulnerabilities and deployment challenges. Stakeholders must adopt multi-layered security frameworks that integrate advanced encryption, continuous monitoring, strict access control, and proactive threat detection. Key recommendations are listed in Table 7 and they include:

1. Advanced Encryption Techniques: End-to-end encryption and cryptographic key pair mechanisms protect sensitive user and network data. Safeguarding identifiers such as IMSI and UE IDs prevents exploitation if intercepted. Integration with established libraries, such as OpenSSL, strengthens encryption, key management, and overall network security [4].
2. Regular Security Audits and Continuous Monitoring: Frequent audits of physical and digital components—including UEs, base stations, and core networks—enable early vulnerability detection. Real-time monitoring tools allow rapid responses to potential breaches [22].
3. Robust Access Control Mechanisms: Multi-factor authentication for devices, role-based access for administrators, and network slice segmentation minimize exposure to attacks. Ensuring UE security prevents unauthorized access or manipulation [35].
4. Collaboration Across Stakeholders: Effective network security relies on cooperation among equipment manufacturers, service providers, and regulators. Manufacturers must embed security in design, providers enforce policies consistently, and regulators establish clear standards [4].
5. User Education and Awareness: Human error remains a critical risk. Training programs that raise awareness of identity spoofing, manipulated behaviour, and other threats reduce vulnerability [22].

Table 7. Key Vulnerabilities in Private 5G Networks and Future Research Directions.

Vulnerability	Description/Impact	Future Research Directions
DDoS attacks	Overload network resources, disrupting mission-critical services.	Develop resilient traffic filtering, AI-driven anomaly detection, and real-world validation of scalable mitigation strategies.
Spoofing	Impersonation of devices/users to gain unauthorized access.	Stronger authentication (e.g., SDP, multi-factor), and adaptive identity verification mechanisms.
Unauthorized access	Exploits weak authentication and access control, worsened by device density.	Role-based access control, continuous monitoring, and empirical studies on long-term effectiveness.
Jamming attacks	Flood communication channels with interference, degrading QoS.	Research on anti-jamming protocols, spectrum agility, and moving target defence.
Man-in-the-Middle (MITM)	Interception and manipulation of communications.	End-to-end encryption, secure handover protocols, and lightweight cryptography for IoT.
Eavesdropping	Intercepts sensitive communications, compromising confidentiality.	Enhanced encryption, privacy-preserving frameworks, and validation in healthcare/IIoT contexts.
Privacy leaks	Unauthorized disclosure of personal or industrial data.	Data governance models, secure data-sharing protocols, and regulatory harmonization.
Tampering	Manipulation of devices or data to disrupt services.	Blockchain-based integrity verification and intrusion-tolerant orchestration.
Fake base stations	Rogue nodes intercept communications and harvest data.	Secure base station authentication, anomaly detection, and cross-layer defence models.

In essence, the secure operation of private 5G networks requires a combination of technical, organizational, and human measures. Integrating these practices strengthens resilience against evolving threats and ensures reliable network operation.

7.1.2. Future Research Directions

Despite growing research on 5G, substantial gaps remain regarding security challenges specific to private 5G networks. Unlike public networks, private deployments in industrial automation, healthcare, or campus environments introduce distinct security risks that require tailored investigation.

Key research directions include:

1. Specific Vulnerabilities in Private Deployments: Case studies are necessary to evaluate encryption, IDPS, and MFA performance in private 5G contexts. Industrial deployments may face attacks targeting network slicing or jamming, while campus networks are vulnerable to internal threats or misconfigurations.
2. Standardized Security Protocols: Private networks operate under diverse regulatory and sector-specific constraints. Developing frameworks that incorporate dynamic access control, edge monitoring, and secure IoT integration is essential to improve resilience and align with operational objectives.
3. Emerging Technologies: AI and ML provide real-time threat detection and adaptive responses but also introduce risks such as adversarial attacks. Future studies should explore AI-driven anomaly detection and secure ML model deployment for private 5G networks.
4. Additional Research Opportunities:
    - Threat Modelling: Limited use of attack graphs exists for private 5G networks. Expanding this approach can enhance vulnerability assessment and mitigation.

- Moving Target Defence (MTD): Dynamic network configurations could increase attack complexity; feasibility studies are needed.
- Automation of Security Models: Automating attack graph generation can accelerate vulnerability identification and response.
- Comparative Security Insights: Studies comparing private 5G, legacy networks, Wi-Fi, public 5G, and SNPNs can inform best practices.

Addressing these gaps will enhance understanding and mitigation of vulnerabilities unique to private 5G, supporting the secure deployment of mission-critical applications across multiple sectors.

8. Conclusions

This review paper offers a comprehensive examination of security vulnerabilities in private 5G networks, addressing key research questions and mapping the current state of knowledge. The study underscores the pressing need for tailored security measures that account for the distinctive characteristics of private 5G deployments, which support mission-critical applications across industrial IoT, healthcare, and smart city infrastructures. Critical vulnerabilities identified include network slicing exploitation, weak or inconsistent authentication mechanisms, challenges associated with edge computing, and threats to data confidentiality, integrity, and availability (CIA). These risks—ranging from unauthorized access and man-in-the-middle attacks to data tampering and AI-driven exploits—pose substantial operational, financial, and reputational consequences, highlighting the imperative for robust mitigation strategies.

The review further identifies several promising countermeasures, such as advanced encryption protocols, AI-powered intrusion detection systems, multi-factor authentication, and blockchain-based identity management. However, practical challenges remain, including scalability limitations, latency constraints, and vulnerabilities inherent to AI-driven systems. These considerations emphasize the necessity for adaptive, context-aware, and multi-layered security frameworks capable of addressing the dynamic and heterogeneous nature of private 5G environments. Significant gaps in the literature are also apparent. These include the scarcity of private 5G–specific security frameworks, limited empirical validation of proposed mitigation strategies, and the underrepresentation of case studies assessing real-world effectiveness. Addressing these gaps is crucial for translating theoretical solutions into operationally viable defenses and for informing evidence-based best practices.

In conclusion, safeguarding private 5G networks demands an integrated approach that combines technical solutions, organizational policies, and human-centric strategies. By synthesizing vulnerabilities, highlighting mitigation measures, and proposing future research directions, this review establishes a foundation for advancing resilient and secure private 5G deployments. As these networks continue to proliferate across mission-critical sectors, the insights presented here provide essential guidance for researchers, practitioners, and policymakers in developing next-generation security solutions capable of anticipating and mitigating evolving threats.

Author Contributions: Conceptualization, J.F. and J.A.G.; methodology, J.F.; validation, J.F., J.A.G. and Y.D.; formal analysis, J.F.; investigation, J.F.; writing—original draft preparation, J.F.; writing—review and editing, J.F., J.A.G., Y.D.; visualization, J.F.; supervision, J.A.G.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data was created during this study.

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

References

1. Ji, S.; Garg, A.K.; Mishra, A.K. *5G Network Implementation: A Survey on Security Issues, Challenges, and Future Directions*; IGI Global Scientific Publishing: Hershey, PA, USA, 2024; pp. 62–88. [CrossRef]
2. Ficzere, D.; Soos, G.; Varga, P. A compact 5G Non-Public Network. In Proceedings of the 2021 17th International Conference on Network and Service Management (CNSM), Izmir, Turkey, 25–29 October 2021.
3. Bhosale, K.S.; Nenova, M.; Iliev, G. A study of cyber attacks: In the healthcare sector. In Proceedings of the 2021 Sixth Junior Conference on Lighting (Lighting), Gabrovo, Bulgaria, 23–25 September 2021.
4. Alanazi, M.N. 5G Security Threat Landscape, AI and Blockchain. *Wirel. Pers. Commun.* **2023**, *133*, 1467–1482. [CrossRef]
5. Aijaz, A. Private 5G: The Future of Industrial Wireless. *IEEE* **2020**, *14*, 136–145. [CrossRef]
6. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. 5G security: Analysis of threats and solutions. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017.
7. Wen, M.; Li, Q.; Kim, K.J.; Lopez-Perez, D.; Dobre, O.A.; Poor, H.V. Private 5G Networks: Concepts, Architectures, and Research Landscape. *IEEE* **2022**, *16*, 7–25. [CrossRef]
8. Tripathi, A.; Thakur, A.; Tamma, B.R. Attack Graphs for Standalone Non-Public 5G Networks. In Proceedings of the 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 10–14 October 2022.
9. Eswaran, S.; Honnavalli, P. Private 5G networks: A survey on enabling technologies, deployment models, use cases and research directions. *Telecommun. Syst.* **2023**, *82*, 3–26. [CrossRef]
10. Mangla, C.; Rani, S.; Qureshi, N.M.F.; Singh, A. Mitigating 5G security challenges for next-gen industry using quantum computing. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 101334. [CrossRef]
11. Chin, H.-H.; Lin, H.-C.; Cheng, Y.-C.; Tsai, C.-Y. Development status of 5G private networks in taiwan: Law and practice. *Wirel. Netw.* **2023**, *30*, 6833–6850. [CrossRef]
12. Ahokangas, P.; Matinmikko-Blue, M.; Yrjölä, S.; Hämmäinen, H. Platform configurations for local and private 5G networks in complex industrial multi-stakeholder ecosystems. *Telecommun. Policy* **2021**, *45*, 102128. [CrossRef]
13. Ahad, A.; Ali, Z.; Mateen, A.; Tahir, M.; Hannan, A.; Garcia, N.M.; Pires, I.M. A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions. *Array* **2023**, *18*, 100290. [CrossRef]
14. Maman, M.; Calvanese-Strinati, E.; Dinh, L.N.; Haustein, T.; Keusgen, W.; Wittig, S.; Schmieder, M.; Barbarossa, S.; Merluzzi, M.; Costanzo, F.; et al. Beyond private 5G networks: Applications, architectures, operator models and technological enablers. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 195. [CrossRef] [PubMed]
15. Adil, M.; Song, H.; Khan, M.K.; Farouk, A.; Jin, Z. 5G/6G-enabled metaverse technologies: Taxonomy, applications, and open security challenges with future research directions. *J. Netw. Comput. Appl.* **2024**, *223*, 103828. [CrossRef]
16. Karaagac, A.; Dobrijevic, O.; Schulz, D.; Seres, G.; Nazari, A.; Przybysz, H. Managing 5G Non-Public Networks from Industrial Automation Systems. In Proceedings of the 2023 IEEE 19th International Conference on Factory Communication Systems (WFCS), Pavia, Italy, 26–28 April 2023.
17. Kim, W.; Kim, K.; Lee, J.; Park, H. 5G Architecture Based on Software-Defined Perimeter (SDP) for Direct Trust Access to Private Networks. In Proceedings of the 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA, 24–27 July 2023; pp. 2719–2721. [CrossRef]
18. Lackner, T.; Hermann, J.; Dietrich, F.; Kuhn, C.; Angos, M.; Jooste, J.L.; Palm, D. Measurement and comparison of data rate and time delay of end-devices in licensed sub-6 GHz 5G standalone non-public networks. *Procedia CIRP* **2022**, *107*, 1132–1137. [CrossRef]
19. Nimkar, V.C.; Pingle, S.A.; Bhagat, K.N. Private 5G, "Not As Private As You May Think". *J. Adv. Zool.* **2023**, *44*, 73–78. [CrossRef]
20. Sarakis, L.; Trakadas, P.; Martrat, J.; Prior, S.; Trullols-Cruces, O.; Coronado, E.; Centenaro, M.; Kontopoulos, G.; Atxutegi, E.; Gkonis, P.; et al. Cost-Efficient 5G Non-Public Network Roll-Out: The Affordable5G Approach. In Proceedings of the IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 7–10 September 2021; pp. 221–227. [CrossRef]
21. Corici, M.; Chakraborty, P.; Magedanz, T.; Gomes, A.S.; Cordeiro, L.; Mahmood, K. 5G Non-Public-Networks (NPN) Roaming Architecture. In Proceedings of the 2th International Conference on Network of the Future (NoF), Coimbra, Portugal, 6–8 October 2021.
22. Djuitcheu, H.; Mallikarjun, S.B.; Habibi, M.A.; Kuruvatti, N.P.; Schotten, H.D. Securing Private 5G Campus Networks: Abstract Survey on Current Status, Security Threats, and Research Landscape. In Proceedings of the 2023 2nd International Conference on 6G Networking (6GNet), Paris, France, 18–20 October 2023.
23. Angin, P.; Atalay, M.; Gokce, F.C.; You, I. A Survey on the Security of European 5G Private Networks. *Res. Briefs Inf. Commun. Technol. Evol.* **2022**, *8*, 162–181. [CrossRef]

24. Wani, M.; Horstmann, T.; Kretschmer, M. Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. *J. Cybersecur. Priv.* **2024**, *4*, 23–40. [CrossRef]
25. Cui, Z.; Cui, B.; Su, L.; Du, H.; Xu, J.; Fu, J. A formal security analysis of the fast authentication procedure based on the security context in 5G networks. *Soft Comput.* **2024**, *28*, 1865–1881. [CrossRef]
26. Lin, C.-C.; Tsai, C.-T.; Liu, Y.-L.; Chang, T.-T.; Chang, Y.-S. Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges. *Mob. Netw. Appl.* **2023**, *28*, 1043–1058. [CrossRef]
27. Suraci, C.; Araniti, G.; Abrardo, A.; Bianchi, G.; Iera, A. A stakeholder-oriented security analysis in virtualized 5G cellular networks. *Comput. Netw.* **2021**, *184*, 107604. [CrossRef]
28. Alwahaishi, S.; Zdrálek, J. Biometric Authentication Security: An Overview. In Proceedings of the 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bengaluru, India, 4–7 November 2020.
29. Frank, H.; Meixner, C.C.; Assis, K.D.R.; Yan, S.; Simeonidou, D. Techno-Economic Analysis of 5G Non-Public Network Architectures. *IEEE Access* **2022**, *10*, 70204–70218. [CrossRef]
30. Pavan, G.V.; Meeradevi; Sangeetha, V. Survey on Security Risks in 5G Private Industrial Networks. In Proceedings of the 2022 4th International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, 21–23 December 2022.
31. Liu, I.-H.; Lee, M.-H.; Li, J.-S. Securing 5G Non-Public Networks Against Fake Base Station. *J. Robot. Netw. Artif. Life* **2023**, *10*, 156–159.
32. Altaleb, H.; Zoltán, R. Addressing Cybersecurity Challenges in 5G-enabled IoT and Critical Infrastructures: A Comprehensive Overview. In Proceedings of the 2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES), Nairobi, Kenya, 26–28 July 2023.
33. Ramezanpour, K.; Jagannath, J.; Jagannath, A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. *Comput. Netw.* **2022**, *221*, 109515. [CrossRef]
34. Prados-Garzon, J.; Ameigeiras, P.; Ordonez-Lucena, J.; Muñoz, P.; Adamuz-Hinojosa, O.; Camps-Mur, D. 5G Non-Public Networks: Standardization, Architectures and Challenges. *IEEE Access* **2021**, *9*, 153893–153908. [CrossRef]
35. Hasan, M.K.; Ghazal, T.M.; Saeed, R.A.; Pandey, B.; Gohel, H.; Eshmawi, A.A.; Abdel-Khalek, S.; Alkhassawneh, H.M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Commun.* **2021**, *16*, 421–432. [CrossRef]
36. Javed, M.A.; Niazi, S.K. 5G Security Artifacts (DoS/DDoS and Authentication). In Proceedings of the 2019 International Conference on Communication Technologies, Rawalpindi, Pakistan, 20–21 March 2019.
37. Gaber, T.; Jazouli, Y.E.; Eldesouky, E.; Ali, A. Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges. *Electronics* **2021**, *10*, 1357. [CrossRef]
38. Kitchin, R.; Dodge, M. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *J. Urban Technol.* **2017**, *26*, 47–65. [CrossRef]
39. Lackner, T.; Jooste, J.L.; Palm, D. Decision-support framework to evaluate the practicality of 5G for intralogistics use cases in standalone non-public networks. *Procedia CIRP* **2023**, *120*, 51–56. [CrossRef]
40. Mejia, N.A.; Perelló, J.; Santos-Boada, G.; Amazonas, J.R.d.A. A Multidisciplinary Model to Quantify Human Uncertainty in Human-Centric Cyber-Physical-Social Systems: A 5G Application Use Case. *IEEE Access* **2024**, *12*, 63484–63503. [CrossRef]
41. Pirayesh, H.; Zeng, H. Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 767–809. [CrossRef]
42. Badhwar, R. Man-in-the-Middle Attack Prevention. In *The CISO's Next Frontier*; Springer: Cham, Switzerland, 2021. [CrossRef]
43. Mazroa, A.A.; Arozullah, M. Securing the User Equipment (UE) in LTE Networks by Detecting Fake Base Stations. *Int. J. Soft Comput. Eng.* **2015**, *4*, 94–97.
44. Purification, S.; Wuthier, S.; Kim, J.; Kim, J.; Chang, S.-Y. Fake Base Station Detection and Blacklisting. In Proceedings of the 2024 33rd International Conference on Computer Communications and Networks (ICCCN), Kailua-Kona, HI, USA, 29–31 July 2024.
45. Chakraborty, P.; Corici, M.; Zope, H.; Barjau, C.; Awan, M.F.; Ribes, J. A Framework for Roaming between 5G Non-Public-Networks (NPNs). In Proceedings of the 2023 IEEE Conference on Standards for Communications and Networking (CSCN), Munich, Germany, 6–8 November 2023.
46. Ordóñez, J.A.; Folgueira, J.; Contreras, L.M.; Pastor, A. The use of 5G Non-Public Networks to support Industry 4.0 scenarios. In Proceedings of the 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 28–30 October 2019.
47. Mohan, J.P.; Sugunaraj, N.; Ranganathan, P. Cyber Security Threats for 5G Networks. In Proceedings of the 2022 IEEE International Conference on Electro Information Technology (EIT), Mankato, MN, USA, 19–21 May 2022.