A Systematic Literature Review:

Security Vulnerabilities in Private 5G Networks: Challenges and Mitigation Strategies

Jacinta Fue

A thesis submitted to the Faculty of Design and Creative Technologies Auckland University of Technology

In partial fulfilment of the requirements for the degree of
Master of Cyber Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand, 14 February 2025

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

…….

Jacinta Fue

14 February 2025

Acknowledgements

I would like to thank my supervisor, Dr Jairo Gutierrez, for providing guidance and support throughout my thesis. I would also like to thank Dr Alastair Nisbet who leading up to this thesis gave me advice and encouragement for which I am truly grateful.

I would like to express my deepest gratitude to my parents, Savali & Lusia Chan Foung, whose endless sacrifices have provided me with the opportunity to build a bright future. Their steadfast support and guidance, along with the values they instilled in me, faith, gratitude, and kindness, have shaped the person I am today.

To my two beautiful children Jhosiah and Zuko, thank you for allowing me to dedicate weekends and evenings to my studies, allowing me to sacrifice family time. You have both been my rock, reminding me that anything is possible with hard work and perseverance.

Finally, to my husband, Rueben, thank you for always encouraging me to pursue my goals and reach my full potential. Your unwavering support, willingness to take care of our family while I studied, and belief in me made this journey possible. Without you, I could not have followed my newfound passion for learning and completed this thesis.

Table of Contents

Abstract

As industries demand ultra-dependable, low-latency connectivity, private fifth generation (5G) networks have emerged as a critical solution. Unlike conventional technologies such as 4G or Wi-Fi, private 5G networks offer tailored advantages, including guaranteed service continuity, enhanced reliability, and customizable security features. These networks are particularly valuable in sectors such as industrial automation, healthcare, and smart cities, where stringent security, privacy, and performance requirements are paramount. Despite their advantages, private 5G networks introduce significant security challenges, particularly concerning the confidentiality, integrity, and availability of data and services. This thesis investigates security vulnerabilities in private 5G networks through a systematic literature review (SLR). It identifies the key challenges associated with deploying and managing private 5G networks, analysing the risks they introduce. Additionally, the study examines existing strategies and mitigation approaches discussed in the literature. Furthermore, it highlights research gaps and suggests potential directions for future studies to enhance the security of private 5G networks.

Keywords

Private 5G Network, Non-Public 5G Networks, Standalone Non-Public Networks (SNPNs), 5G Network Security Challenges, Security Vulnerabilities in Private 5G Networks

1.Introduction

In recent years, the rapid growth of innovative technologies, especially in cloud computing, has transformed both public and private sectors(Ji et al., 2024). This surge, in turn, has spurred a heightened demand for enhanced communication infrastructures characterized by advanced capabilities, expedited connectivity, and elevated data transmission rates. As technology advances, the rate of network security attacks has skyrocketed, targeting individuals, businesses, and critical industries such as healthcare and finance (Ficzere et al., 2021). As a result, in industries like healthcare, network security breaches can have far-reaching and potentially catastrophic effects. Beyond the immediate risk of exposing sensitive patient data, such breaches can paralyse critical medical systems, severely disrupting the delivery of care (Bhosale et al., 2021). For instance, a ransomware attack could infiltrate a hospital's network and lock down electronic health records (EHRs), preventing healthcare professionals from accessing vital patient information such as medical histories, lab results, or prescribed medications(Bhosale et al., 2021). This lack of access creates delays in treatment, increasing the risk of misdiagnoses or incorrect treatments, which could lead to life-threatening consequences.

Moreover, the impact extends beyond patient care. Various types of attacks can lead to distinct consequences, such as unauthorized access, data breaches, and financial losses. Organizations, including those in healthcare, are particularly vulnerable to these financial impacts, making it crucial to understand these risks in order to prioritize effective defence strategies(Alanazi, 2023). Breaches often require costly legal actions, forensic investigations, and system restorations. In 5G-based smart healthcare networks, while enhanced capabilities are offered through cloud resources, they also face unique security challenges. For example, threats such as Distributed Denial of Service (DDoS) attacks and jamming attacks disrupt critical network functions, including network slicing and radio access, compromising the reliability of healthcare services(Ahad et al., 2023).

The financial and reputational damage caused by these security breaches can be immense(Ahad et al., 2023). Loss of trust can significantly impact the adoption and effectiveness of private 5G networks, leading to negative consequences for organizations. Beyond the risk of data exposure, cyberattacks targeting private 5G networks can disrupt authentication processes between devices and network infrastructure, causing communication failures. Authentication plays a crucial role in verifying the identities of users and devices within these networks(Wen et al., 2022). Primary authentication facilitates mutual authentication between devices and networks, though challenges such as inadequate device support and insufficient knowledge control remain. To enhance security, secondary authentication, based on standards like the 3GPP framework, can further protect communications beyond the operator domain through protocols such as the Extensible Authentication Protocol (EAP)(Tripathi et al., 2022).

As mentioned in "A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions"(Ahad et al., 2023), Confidentiality and integrity protection are also crucial for ensuring that only authorized personnel can access sensitive data and that this data remains secure during transmission. In 5G networks, encryption mechanisms have a fundamental role in securing data during transmission, guaranteeing its confidentiality and strengthening overall network security (Alanazi, 2023). However, due to the resource limitations of IoT devices commonly used in various industries, specialized protocols are required to maintain network integrity without overwhelming these devices. Security breaches compel organizations to divert critical resources, both financial and human, away from their core operations and into cybersecurity recovery efforts, hindering their ability to maintain efficiency and deliver quality services (Ahad et al., 2023).

Cybercriminals can exploit vulnerabilities in critical infrastructure, financial systems, and private data, leading to severe financial losses, privacy breaches, and disruptions to essential services. These attacks, ranging from ransomware to sophisticated phishing schemes and distributed denial-of-service (DDoS) assaults, affect not only large corporations but also small businesses and everyday users, creating a ripple effect across society(Ahmad et al., 2017). The growing digital dependence has made robust network security a vital defence for safeguarding sensitive information and maintaining public trust 5G technology offers several benefits that can have a vast contribution to various aspects of society, industries, and technology in a significant way. Primarily it offers notably faster data transfer speeds, minimising delays with lower latency, expands network capacity, improved reliability and seamless connectivity between devices enabling more efficient industries and cities(Aijaz, 2020). Overall, the benefits of 5G technology extend far beyond what people's expectations have traditionally envisioned, spurring a shift in connectivity, innovation, and societal progress.

As the demand for faster speeds and seamless connectivity continues to grow (Eswaran & Honnavalli, 2023), so does the need for organizations to establish their own customized security guidelines and infrastructure, which public telecommunications networks cannot adequately provide. Private 5G networks, also known as Non-Public Networks (NPN), offer organizations the opportunity to create their own dedicated network that can be independently managed. A private 5G network is a standalone system designed for exclusive use by a corporation or business, providing numerous benefits including improved coverage in remote areas, enhanced reliability in indoor spaces, and superior data security(Eswaran & Honnavalli, 2023). While private 5G networks offer the same fundamental capabilities as public 5G, their distinct advantage lies in the organisation's ability to control security policies, data management, and service configurations.

Furthermore, 5G networks have the potential to revolutionise numerous industries and enterprises, driving advancements toward increased autonomy and self-sufficiency while enhancing the quality of service (QoS) (Mangla et al., 2023). Public 5G networks, owned and managed by telecommunications operators, face significant challenges such as high energy consumption and the need for extensive coverage. Public mobile network operators often prioritise network deployment in densely populated areas to mitigate deployment costs, resulting in inadequate network coverage in less residential regions. Additionally, coverage can be suboptimal in indoor locations, further complicating communication and connectivity (Mangla et al., 2023). These limitations underscore the value of private 5G networks, which can offer tailored solutions to meet specific organisational needs and overcome the challenges associated with public network infrastructure.

However, the adoption of private 5G networks, while offering several advantages, also introduces a host of security challenges and issues that must be addressed to ensure their successful deployment and operation (Eswaran & Honnavalli, 2023). This thesis will examine the various security risks associated with private 5G or Non-Public Networks (NPN), providing a comprehensive analysis of the potential vulnerabilities and threats that organizations may face. Additionally, this thesis will explore the security issues and challenges that have emerged throughout the lifecycle of mobile network generations, starting from the inception of 1G through the evolution to 5G. Each generation has brought its own set of security concerns, and understanding these historical challenges is crucial for contextualising the current and future risks associated with private networks. By tracing the development of mobile network security from 1G to 5G, this thesis will highlight the persistent and emerging threats, and how these issues are exacerbated or mitigated in the context of private 5G networks. Finally, the analysis section, will delve into the specific security challenges inherent in private 5G networks, offering insights into how organisations can better safeguard their data and operations in an increasingly connected and digital world.

1.1Motivation

The motivation for this research arises from the growing need to understand and address the security vulnerabilities associated with the implementation and operation of private 5G networks. As industries increasingly rely on 5G technology for mission-critical applications, ensuring the confidentiality, integrity, and availability of data and services becomes paramount. This thesis is driven by an extensive review of prior studies in the field of telecommunications, with a specific focus on wireless communication networks.

The research investigates four key areas:

1. Security Vulnerabilities and Operational Issues: The thesis examines the wide range of security vulnerabilities and operational challenges in private 5G networks during both their implementation and ongoing operation. By providing a thorough analysis of these vulnerabilities, the goal is to offer a comprehensive understanding of the risks involved in deploying and managing private 5G infrastructure. This section will contribute to existing knowledge on network security, identifying crucial areas for strengthening the resilience of private 5G networks in diverse operational environments.

2. Risks to Data and Service Confidentiality, Integrity, and Availability: The thesis highlights how the identified threats may jeopardise the confidentiality, integrity, and availability of data and services in private 5G networks. A detailed exploration of these risks is essential for understanding the specific security challenges faced by private 5G systems and provides a foundation for addressing these vulnerabilities.

3. Mitigation Strategies: A key motivation of this thesis is to examine proposed mitigation strategies suggested by academics and industry researchers. Given the multitude of security challenges facing private 5G networks, this research seeks to synthesise these proposed solutions and offer insights into effective risk mitigation approaches. The aim is to reinforce the security posture of private 5G networks and contribute to ongoing efforts to enhance their resilience against cyber threats.

4. Identifying Gaps and Future Research: This thesis also aims to identify gaps in the existing literature on private 5G network security. By highlighting areas that have not been adequately addressed, this research will uncover opportunities for further investigation and development. The findings will guide future research efforts, enabling stakeholders to focus on critical areas that need further attention.

By investigating these key areas, this thesis will provide valuable insights into the unique security vulnerabilities and risks associated with private 5G networks.

1.2 Problem Statement

Private 5G networks are becoming increasingly popular across various industries due to their ability to provide enhanced connectivity, reliability, and greater control tailored to specific enterprise needs (Lackner et al., 2022). These networks are particularly leveraged in critical environments such as healthcare, manufacturing, and smart cities, where the protection of data integrity, confidentiality, and availability is paramount. In such settings, ensuring that sensitive data is kept secure while maintaining the highest levels of operational efficiency is essential. However, despite the many advantages that private 5G networks offer, they also present a range of security challenges. One of the key issues lies in the expanded attack surface created by the integration of IoT devices, the reliance on network slicing, and the deployment of edge computing technologies(Mangla et al., 2023). These factors increase the complexity of the network and introduce new vulnerabilities. Additionally, the

coexistence of private 5G networks with legacy systems, combined with the potential for insider threats, further exacerbates the security risks(Tripathi et al., 2022). As the deployment of private 5G networks becomes more widespread in critical sectors, they become increasingly attractive targets for cyber attackers, who seek to exploit vulnerabilities to gain unauthorized access, disrupt operations, or steal sensitive data.

Most 5G security research targets public networks, leaving a gap in understanding private 5G security challenges. This gap underscores the urgent need to identify, analyse, and mitigate the specific vulnerabilities associated with private 5G networks to protect critical assets and ensure the continuity of operations. The purpose of this thesis is to conduct a systematic literature review (SLR) to identify, analyse, and categorize the security vulnerabilities present in private 5G networks. Through a comprehensive examination of the existing literature, this research aims to provide an in-depth understanding of the current security landscape in private 5G environments, highlight potential risks, and propose strategies for mitigating these vulnerabilities. The outcomes of this research will contribute to enhancing the security posture of private 5G networks and offer valuable insights for guiding future research and development in this area.

2. Background

2.1 Evolution of Mobile Network Security

The progression from 1G to 5G in mobile communication represents an ongoing journey of technological advancement, continuously reshaping the way we connect with the world(Vij & Jain, 2016). Each mobile generation has introduced new capabilities, pushing boundaries and redefining what is possible in terms of connectivity and security. In the early 1980s, 1G marked the beginning of mobile communication by introducing analogue transmission primarily for voice services(Angin et al., 2022). Although groundbreaking at the time, 1G networks were notorious for their lack of encryption, making voice conversations vulnerable to interception. Additionally, 1G had minimal authentication mechanisms, making it susceptible to impersonation and fraud. The network was designed for voice communication, and consequently, security protocols were underdeveloped, leaving it exposed to a variety of threats(Vij & Jain, 2016).

With the arrival of 2G in the early 1990s, mobile communication saw a shift to digital transmission, improving security through encryption (Eluwole et al., 2018). However, 2G still had significant flaws, such as weak encryption standards and a lack of mutual authentication between users and the network. These vulnerabilities made the network susceptible to spoofing attacks and left communication channels insecure, allowing threats like eavesdropping and interception to flourish (Mangla et al., 2023). The introduction of 3G included enhanced encryption protocols and improvements in user authentication, addressing weaknesses observed in 2G. Nonetheless, 3G was not without its own vulnerabilities(Vij & Jain, 2016). Despite its stronger security measures, 3G was still receptive to attacks which allowed attackers to manipulate data sessions. Furthermore, with the expansion of data services, new concerns such as data leakage emerged, highlighting the need for more robust protection mechanisms to secure increasingly sensitive information.

The launch of 4G ushered in new capabilities, including faster data speeds and better support for multimedia applications. Despite these advancements, security challenges persisted, especially with the introduction of technologies like network slicing and virtualization (Suraci; et al., 2021). These innovations presented new challenges, such as ensuring isolation between different network slices and preventing unauthorized access. Additionally, the increase in data services and applications expanded the attack surface, making networks more vulnerable to threats such as Distributed Denial of Service (DDoS) attacks and malware.

2.2 Overview of 5G Technology

Wireless communication has undergone significant evolution over the past three decades, fundamentally transforming how people and devices connect. This began with the introduction of 1G in the 1980s, which relied on analogue technology to deliver basic public voice services. While groundbreaking at the time, 1G had numerous limitations, including poor call quality, low capacity, frequent call drops, and susceptibility to interference(Shukurillaevich et al., 2019). Security was also a major concern, as 1G networks lacked encryption, making calls vulnerable to eavesdropping(Shukurillaevich et al., 2019). Additionally, the bulky size of devices and short battery life further restricted its practicality. These shortcomings highlighted the urgent need for technological improvements. With the arrival of 2G, wireless communication underwent a transformative shift through the introduction of digital transmission, which significantly enhanced voice quality and added new services like SMS and MMS(Adebusola et al., 2020). Security improved with the inclusion of encryption and authentication mechanisms, addressing the vulnerabilities of 1G. Global roaming became possible, fostering greater connectivity worldwide. Despite these advancements, 2G was not without its flaws. Issues such as dropouts being experienced under bad conditions, weak signals and

having a jagged steppy curve(Bhandari et al., 2017). These limitations exposed the need for stronger security protocols and more reliable network designs.

3G built upon the successes of 2G by delivering broadband and multimedia services, enabling faster internet access and better support for applications such as global roaming and enhanced voice quality. However, 3G came with its own set of drawbacks, its scope was very restricted and was not reliable(Bhandari et al., 2017). Additionally, the cost of setting up and maintaining 3G infrastructure was higher, making it less economical compared to earlier generations(Adebusola et al., 2020). These inefficiencies called for a more energy-efficient and cost-effective solution, paving the way for the next generation of wireless technology. 4G marked a revolutionary leap in mobile communication by prioritizing high-speed data transmission and seamless integration of voice, multimedia, and internet services(Adebusola et al., 2020). Its architecture, which utilized advanced techniques like MIMO, carrier aggregation, and interference mitigation, provided superior Quality of Service (QoS). However, the introduction of 4G also came with its challenges. The growing complexity of managing heterogeneous networks increased operational demands(Bhandari et al., 2017). Additionally, while advancements were made to address energy efficiency, achieving higher capacity and supporting the explosive growth of connected devices remained bottlenecks(Bhandari et al., 2017).

Despite their limitations, these successive generations collectively laid the foundation for modern wireless communication. The incremental improvements, along with the lessons learned from their disadvantages, set the stage for the development of 5G. Now, the fifth generation of wireless technology, or 5G, has emerged as a game-changer, offering unprecedented capabilities such as ultra-fast speeds, reduced latency, and enhanced network coverage(Aijaz, 2020). Unlike its predecessors, 5G is specifically designed to address the growing demands of modern communication networks, including the Internet of Things (IoT), autonomous systems, and smart city infrastructure(Alanazi, 2023). Its advanced architecture supports a higher density of connected devices, enabling seamless video streaming and real-time data processing, which are critical for applications like autonomous vehicles, remote healthcare, and augmented reality(Aijaz, 2020). Moreover, 5G networks deliver larger coverage areas and improved Quality of Service (QoS), ensuring consistent and reliable connectivity even in densely populated areas.

These advancements represent not merely an iterative improvement, but a shift in how wireless networks is designed and utilized. By enabling cutting-edge technologies and providing the infrastructure for next-generation applications, 5G is poised to become the backbone of future technological innovation (Aijaz, 2020). The architectural improvements of 5G, such as network slicing and edge computing, further enhance its utility across diverse applications. Network slicing enables the creation of multiple virtual networks operating on the same physical infrastructure, each tailored to meet specific use case requirements(Aijaz, 2020). However, alongside its benefits, 5G also introduces significant challenges, particularly in the context of private 5G networks. Unlike public 5G networks, private 5G networks are deployed within organizations to meet specific operational needs(Eswaran & Honnavalli, 2023). They offer greater control, reliability, and customization, making them ideal for industries with stringent requirements, such as mining, logistics, and healthcare. Despite these advantages, the unique architecture of private 5G networks presents new security challenges. Features like network slicing and open interfaces, while advantageous for operational flexibility, also introduce potential vulnerabilities that could be exploited by malicious actors(Lackner et al., 2023). For example, inadequate isolation between network slices may lead to data breaches, while open interfaces could become entry points for attacks(Tripathi et al., 2022).

The growing reliance on private 5G networks for critical infrastructure amplifies the need to address these vulnerabilities. This rapid adoption often outpaces the development and implementation of

robust security measures, leaving private 5G networks susceptible to threats such as denial-of-service (DoS) attacks, eavesdropping, and spoofing(Ahad et al., 2023). These risks are particularly concerning in industries where private 5G networks support high-security environments, such as industrial automation, smart grids, and mission-critical systems (Ficzere et al., 2021). Despite the importance of securing private 5G networks, existing research addressing their specific vulnerabilities remains limited. While public 5G security has been explored extensively, the unique risks associated with private 5G implementations have received comparatively little attention(Tripathi et al., 2022). Table 1, was created to show a detailed overview of the evolution of mobile networks, highlighting the key features and advancements introduced with each generation, as well as the challenges that carried over and evolved over time. Each successive generation, from 1G to 4G, laid the groundwork for the innovations that define modern wireless communication. The table illustrates not only the technological leaps made with each network generation but also the persistent challenges such as security concerns, infrastructure limitations, and operational inefficiencies that were gradually addressed, though never fully eliminated. This visualization of network evolution provides a clear context for understanding how past limitations have shaped the current state of 5G and the emerging security considerations for private 5G networks.

Table 1

Evolution of Mobile Network Generations, Key Features, and Challenges

Network Generation	Key Features	Challenges
1G	• Introduced 1980s • Analog mobile phones (Motorola) • Analog voice communication, no data transfer • Analog technology (AMPS) Advanced Mobile Phone Service	• Poor call quality. • Frequent call drops. • Limited capacity. • No encryption; prone to eavesdropping. • Bulky devices; short battery life
2G	• Introduced 1990s • Feature phones (Nokia) • Digital voice, SMS, limited data (up to 64 kbps) • Global System for Mobile Communications (GSM), Code-Division Multiple Access (CDMA	• Interference issues. • Vulnerable to SIM and base station attacks. • Weak encryption (e.g., A5/1). • Limited data capabilities (SMS/MMS only). • Network congestion in high-demand areas.
3G	• Introduced 2000s • Smartphones (Blackberry & iPhone) • Voice, SMS, mobile internet (up to 2 Mbps), video calls • Universal Mobile Telecommunications Service (UMTS), CDMA2000	• High device power consumption. • Expensive deployment and maintenance. • Limited backward compatibility. • Inefficient spectrum use. • Susceptible to spoofing and man-in-the-middle attacks.
4G	• Introduced 2010s • Smartphones (iPhone, Android devices) • High-speed internet, HD video streaming (up to 1 Gbps), mobile apps • Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX	• Complex heterogeneous network management. • Energy efficiency issues at scale. • Increased exposure to cyber threats. • High implementation costs. • QoS challenges in dense or rural areas.
5G	• Introduced 2020s • 5G-enabled smartphones, IoT devices, Augmented and Virtual Reality (AR/VR) • Ultra-high-speed internet (up to 10 Gbps), low latency, IoT,	• Security risks in network slicing and open interfaces. • Slice isolation vulnerabilities. • Scalability concerns with high device density. • High deployment costs.

	smart cities, autonomous vehicles • Millimetre waves (mm Wave), Massive Multiple Input, Multiple Output (MIMO), Beamforming	• Prone to DoS, eavesdropping, and spoofing attacks. • Limited research on private 5G security.

Note. Adapted from "From 1G to 5G, What next", by O.T. Eluwole, Nsikak Udoh, Mike Oluwatayo Ojo and Cindy Okoro, 2018, IAENG International Journal of Computer Science

3. Literature Review

3.1 Private 5G Networks

With the emergence of Industry 4.0 and the Internet of Things (IoT), industries are seeking more advanced connectivity solutions capable of supporting a vast number of devices, providing low latency, and ensuring high reliability(Chin et al., 2023). Private 5G networks are designed to meet these demands, offering dedicated, secure, and uninterrupted communication tailored to the specific needs of businesses and enterprises (Aijaz, 2020). These networks, also known as non-public mobile networks (NPNs), deliver customized and independent connectivity solutions for organizations requiring enhanced security, reliability, and control. Unlike public 5G networks that serve multiple users and are operated by mobile network operators (MNOs), private 5G networks are dedicated to a single entity or enterprise, often confined to a specific location(Aijaz, 2020). This exclusivity makes private 5G networks particularly well-suited for environments where critical infrastructure is in operation, such as manufacturing facilities, hospitals, transportation hubs, airports, seaports, and military bases. In these settings, ensuring data security, minimal latency, and continuous connectivity is of utmost importance(Aijaz, 2020).

Private 5G networks provide organizations with full control over their infrastructure, enabling the customization of security protocols and network configurations to suit their needs(Chin et al., 2023). However, this autonomy comes with significant challenges, such as the need for substantial investment in network infrastructure and the necessity of a skilled IT workforce to manage and maintain the system(Wen et al., 2022). On the other hand, dependent private 5G networks, managed by an MNO, offer businesses scalability and flexibility by shifting the responsibility for network management and security to the operator(Ahokangas et al., 2021). This model is especially attractive to companies looking to outsource network operations, although it may raise concerns about data privacy and control. The MNO is also responsible for the installation of network infrastructure, including both the radio access network (RAN) and core network components. Businesses using this model must ensure that network users are effectively managed, and that the infrastructure remains secure and operational.

For organizations with adequate technical resources, owning and managing the private 5G network is also an option, with internal IT departments overseeing operations. Alternatively, companies can engage system integrators to design and manage the network, allowing them to leverage specialized expertise while reducing the burden on internal resources(Chin et al., 2023). Dependent private 5G networks, in contrast, are fully managed by an MNO, which takes on the responsibility for installation, operation, and maintenance of the network infrastructure(Eswaran & Honnavalli, 2023). This model allows organizations to benefit from the MNO's expertise, operational capabilities, and spectrum licenses. It offers greater scalability and flexibility, as the operator can continuously integrate new features and updates into the network. For businesses seeking to concentrate on their core activities

without the need to heavily invest in network management or acquire specific technical skills, the dependent model provides a suitable alternative. Both types of private 5G networks offer substantial advantages over traditional public networks, including better data security, greater control over network performance, and the ability to tailor services to specific use cases. As industries increasingly adopt IoT, automation, and other advanced technologies, private 5G networks are essential in providing the robust and reliable connectivity needed to support these innovations. Through private 5G, organizations can ensure that their communication needs are met with high security, low latency, and consistent performance, making these networks crucial components of modern industrial and enterprise environments(Wen et al., 2022).

One of the most significant benefits of private 5G networks is the enhanced security they offer. Since these networks are dedicated to specific enterprises, they can be tailored to meet stringent security requirements, including implementing end-to-end encryption, advanced access controls, and segregated traffic flows. For instance, healthcare organizations using private 5G can securely transmit patient data, including medical records and imaging, without the risk of exposure on public networks(Ahad et al., 2023). Private 5G networks also offer compliance advantages, ensuring organizations meet regulatory standards such as GDPR in Europe or HIPAA in the U.S., thereby safeguarding customer and patient data in accordance with applicable laws(Ahokangas et al., 2021). In sectors like manufacturing, private 5G networks support smart factories, enabling real-time machine monitoring and predictive maintenance. In healthcare, private 5G facilitates remote surgeries and high-definition video consultations, where the low latency and high bandwidth ensure real-time communication without compromising data security or quality (Eswaran & Honnavalli, 2023).

As the demand for real-time data processing grows, AI-powered network management and edge computing will play an increasingly vital role in private 5G networks. These technologies will allow for self-optimizing networks that adjust automatically to changing conditions, ensuring optimal performance at all times. Moreover, as we look towards the future of 6G and beyond, private 5G networks will evolve to support even more complex applications, creating new opportunities for industries to push the boundaries of automation and innovation(Adil et al., 2024). Private 5G networks are being adopted across various industries, each leveraging their capabilities to enhance security, operational efficiency, and network reliability. Sectors such as manufacturing, ports, smart cities, healthcare, and educational campuses are among those integrating private 5G to support their unique connectivity needs. These networks provide organizations with greater control over infrastructure while ensuring high-performance communication tailored to their specific operational requirements(Maman et al., 2021). Table 2, "Private 5G Networks Across Different Industries," outlines key sectors adopting private 5G and highlights their applications in enhancing connectivity, security, and efficiency**.**

Table 2

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

3.1.1 Architecture of Private 5G Networks

The architecture of private 5G networks is comprised of several critical components that distinguish them from public networks(Karaagac et al., 2023). At the core of these systems lies the Radio Access Network (RAN), which consists of base stations and antennas that enable wireless communication between user devices and the network. The RAN is essential in providing the radio coverage necessary for devices to connect and communicate with each other within the network. Complementing the RAN, the core network plays a essential role in managing device connectivity, mobility, and routing of data. The core network ensures seamless handover of devices between different base stations and is responsible for enforcing security and network policies. User Equipment (UE), such as smartphones, tablets, and IoT devices, interact with both the RAN and core network to facilitate communication and data transfer across the private 5G network(Kim et al., 2023). These components work in unison to deliver high performance, low latency, and exceptional reliability. Private 5G networks are designed to cater to specific operational requirements, making them particularly suited for organizations that

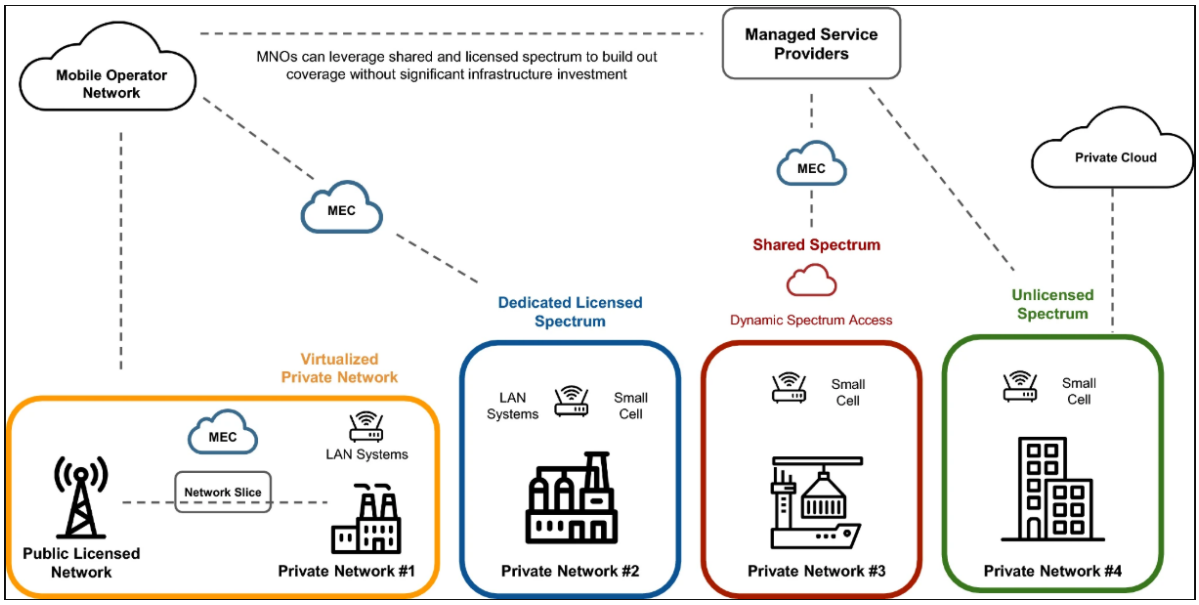
demand a tailored connectivity solution. Unlike public networks, private 5G infrastructures provide businesses with the flexibility to fully customize and control their network, including security features and performance configurations, to meet their unique needs. By allowing such customization, private 5G networks ensure that organizations maintain control over their data traffic and can prioritize specific applications, thereby optimizing network performance(Aijaz, 2020).

Private 5G networks also offer a range of deployment models that further enhance their flexibility and adaptability. These models include standalone and non-standalone configurations(Tripathi et al., 2022). Standalone deployments operate independently of any existing public network infrastructure, providing organizations with complete autonomy over network resources, security protocols, and data management(Lackner et al., 2022). This configuration ensures that businesses have full control over every aspect of their network. In contrast, non-standalone deployments leverage existing public network infrastructure for certain functions, such as traffic routing or coverage extension, while still maintaining dedicated resources for the private network's exclusive use(Nimkar et al., 2023). This hybrid approach allows for cost-effective deployment while still offering the key advantages of private 5G, including enhanced security and low-latency performance(Aijaz, 2020). A critical aspect of the architecture of private 5G networks is the security features integrated into the system. These networks implement advanced encryption protocols, which safeguard the integrity and confidentiality of the data transmitted across the network. Robust authentication mechanisms are employed to prevent unauthorized access and ensure that only legitimate devices and users can connect to the network. Moreover, network slicing is a key feature of private 5G networks. It enables the creation of multiple virtual networks within a single physical infrastructure. Each slice can be configured with distinct security policies, performance characteristics, and resource allocations, ensuring that critical applications or user groups are isolated from others and receive the resources they need without interference(L. Sarakis et al., 2021). This level of flexibility and customization helps mitigate potential security vulnerabilities and provides a secure environment for businesses to deploy mission-critical applications.

In addition, the architecture of private 5G networks is designed to deliver optimal performance and security while offering complete control and flexibility to organizations. The ability to customize the network infrastructure, coupled with advanced security protocols and deployment options, makes private 5G networks ideal for industries with specific, high-priority operational needs. The integration of network slicing and robust authentication methods ensures that these networks are secure, scalable, and adaptable to the demands of modern enterprise environments(Tripathi et al., 2022). Following the discussion of private 5G network architecture, Figure 2.1 provides a visual representation of the core components that make up a private 5G network. This diagram illustrates the relationship between the Radio Access Network (RAN), the core network, and user equipment (UE), highlighting the key elements involved in ensuring seamless communication and high performance within private 5G networks. Figure 1, sourced from Eswaran & Honnavalli (2023), provides a detailed layout that aids in understanding the structural setup and the flow of data across a private 5G network.

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 (2023)

3.2 Research Questions

This SLR aims to explore and synthesize the existing research on the security vulnerabilities and risks associated with private 5G networks. As the adoption of private 5G technology accelerates across various sectors, addressing its unique security challenges has become a critical priority. To guide this review, the following research questions have been formulated:

Q1: What security vulnerabilities are associated with private 5G networks?
This question seeks to identify and categorise the specific security vulnerabilities present in private 5G networks. By analysing studies that document these vulnerabilities, this review will offer a comprehensive understanding of the potential weaknesses that could impact the security and performance of private 5G implementations.

Q2: What types of threats pose risks to the confidentiality, integrity, and availability of data and services in private 5G networks?
This question focuses on identifying the types of cyber threats and attacks that could compromise the core security principles, confidentiality, integrity, and availability (CIA) of private 5G networks. The review will assess how these threats specifically target these fundamental aspects of security within the private 5G infrastructure.

Q3: What mitigation strategies have researchers proposed to address security risks in private 5G networks?
This question will explore the range of mitigation strategies, tools, and practices proposed by researchers to secure private 5G networks. The review will evaluate the effectiveness, feasibility, and limitations of these strategies, providing insights into current best practices and potential areas for improvement.

Q4: What gaps exist in current approaches to mitigating security risks in private 5G networks?
This question aims to identify gaps in the current research on security mitigation strategies for private 5G networks. By examining areas that remain underexplored or inadequately addressed, this review will highlight opportunities for future research and emphasize the need for novel approaches to strengthen the security of private 5G deployments.

These research questions are designed to systematically address the security challenges surrounding private 5G networks. The findings from this review will contribute to a deeper understanding of the vulnerabilities, threats, and mitigation strategies within this emerging area, supporting the development of robust security frameworks for private 5G applications.

3.3 Security in 5G Networks

Based on the findings and vulnerabilities identified in relation to 5G networks, numerous critical issues and concerns have emerged, especially as 5G becomes more widely adopted across industries and sectors. One of the primary regulatory challenges involves the extended time frames required for spectrum allocation (Eswaran & Honnavalli, 2023). The process of acquiring the necessary spectrum for 5G networks can be long and cumbersome, creating delays in deployment and leaving networks vulnerable during the interim (Eswaran & Honnavalli, 2023). Furthermore, the limited availability of affordable spectrum adds to the difficulties in accessing this essential resource(Ahokangas et al., 2021). As 5G networks operate across a broader range of frequencies compared to previous generations, ensuring enough bandwidth to support high-speed, low-latency communications becomes a significant challenge(Corici et al., 2021). The increasing demand for spectrum has resulted in rising costs, making it inaccessible to smaller organizations or specific industries(Wen et al., 2022). Additionally, difficulties with network slicing in both public and private 5G networks present another layer of complexity. Network slicing allows multiple virtual networks to coexist on the same physical infrastructure, each tailored to specific use cases or services. Ensuring proper isolation between slices to prevent cross-slice attacks is a major security concern(Tripathi et al., 2022). Compromising one slice could have ripple effects across other slices, endangering sensitive data or mission-critical services(Tripathi et al., 2022). The speed and cost of the authorization process also pose significant obstacles to effective 5G deployment, as organizations struggle to meet the regulatory requirements necessary to roll out secure and compliant 5G infrastructures.

5G networks are subject to significant risks related to the core security principles of authentication, confidentiality, availability, non-repudiation, and integrity. Alanazi (2023) highlights that the broader attack surface of 5G networks introduces a range of vulnerabilities that can be exploited by malicious actors. These vulnerabilities include distributed denial-of-service (DDoS) attacks, eavesdropping on sensitive communications, tampering with data flows, hijacking sessions, spoofing devices, or users, and jamming radio signals to disrupt services. Additionally, 5G networks are prone to advanced cyberattacks such as man-in-the-middle (MITM) attacks, where an attacker intercepts and potentially alters communications between two parties(Alanazi, 2023). Privacy breaches are another significant concern, particularly given the integration of 5G technology in environments such as smart cities, healthcare systems, and industrial IoT networks. Attackers can exploit these vulnerabilities to gain unauthorized access to sensitive personal or confidential data, raising critical security challenges(Tripathi et al., 2022). Research emphasizes the use of attack graphs as a strategic tool for identifying and addressing these vulnerabilities(Alanazi, 2023). Attack graphs provide a detailed mapping of potential attack pathways, enabling organizations to predict and assess risks comprehensively. By simulating potential attack scenarios, these models allow security teams to better understand vulnerabilities and develop targeted defences(Tripathi et al., 2022). This approach is particularly effective against threats like DDoS and spoofing attacks. DDoS attacks overwhelm networks

with excessive traffic, potentially degrading performance or rendering services unavailable(Corici et al., 2021). Spoofing, meanwhile, involves attackers impersonating legitimate users or devices to gain unauthorized access to the network. By employing attack graphs, organizations can identify these vulnerabilities and implement robust security measures, enhancing the resilience of 5G networks against these prevalent threats (Alanazi, 2023).

Traffic manipulation, a serious concern which involves attackers intercepting and altering data transmissions, which could lead to false information being fed into critical systems, such as those controlling autonomous vehicles or industrial robots(Djuitcheu et al., 2023). DDoS attacks, as previously mentioned, are a major concern due to the sheer scale of devices and connections in 5G networks. By flooding the network with illegitimate traffic, attackers can disrupt services across a wide area, causing significant financial and operational damage. Malware injection into devices and network components is another way attackers can compromise 5G networks, either by directly exploiting vulnerabilities in connected devices or by targeting critical infrastructure like network functions virtualization(NFV)(Djuitcheu et al., 2023). Resource exhaustion, where attackers overload the processing power or memory of network components, can also lead to significant disruptions in service. DNS cache poisoning is a particularly dangerous attack vector, as it allows attackers to redirect users to malicious websites by corrupting the domain name system (DNS) entries stored in cache(Djuitcheu et al., 2023). Privilege escalation, where attackers increase their access rights within a system to gain control over critical functions, and physical theft or destruction of network components, such as base stations or routers, pose additional risks(Djuitcheu et al., 2023).

Ultimately, addressing these challenges will require a combination of robust security measures, proactive monitoring, and continuous adaptation to emerging threats(Wen et al., 2022). As 5G networks evolve and their use cases expand, the need to secure these networks becomes increasingly important. Organizations must adopt a comprehensive approach to security that includes encryption, multi-factor authentication, intrusion detection systems, and regular security audits to ensure that vulnerabilities are identified and mitigated before they can be exploited. Additional concerns include unauthorized access, MITM attacks, rogue base stations, jamming, and SIM card cloning (Djuitcheu et al., 2023). Proposed solutions suggest architectures that enable direct trust access through VPN technologies based on Software-Defined Perimeter (SDP). Risks in 5G private networks include threats to network or communication service availability, information leakage, loss of integrity, authentication issues, network slicing vulnerabilities, and malware attacks. Implementing effective security measures remains challenging due to issues such as keeping up with updates, targeting legacy devices, and attacks using low-cost SDR hardware and open-source software. The ongoing need for developing security standards is evident from problems like insecure channels for encryption keys, missing cryptographic integrity protection, optional security measures, roaming security issues, increased DoS attacks, signalling storms, and vulnerabilities in user devices and operating systems(Chin et al., 2023). Emerging technologies and network solutions, such as disaggregated software RAN, 5G SA Core, RAN sharing, and AI/ML for network optimization, also introduce additional concerns(Chin et al., 2023). Additionally, there is a risk of a false sense of security as new 5G mechanisms are mainly available in 5G Stand-Alone networks, highlighting the need for ongoing validation and integration of security attacks into audit frameworks to track vulnerabilities and mitigation strategies over time(L. Sarakis et al., 2021).

3.4 Summary of Selected Literature

Following the rigorous application of the predefined eligibility criteria, a carefully curated set of articles was finalized for inclusion in this SLR. These studies encompass a diverse range of topics related to security vulnerabilities in private 5G networks, reflecting the evolving nature of research in this

domain. Each selected study was subjected to detailed analysis and synthesis in subsequent stages of the review to ensure its relevance to the research objectives and contribution to the broader discourse on 5G security. The selected literature provides a comprehensive exploration of the security challenges inherent in private 5G networks, addressing critical aspects such as emerging threat vectors, architectural vulnerabilities, and the effectiveness of existing mitigation strategies. By focusing on high-quality studies, this review is anchored in a robust body of evidence that captures the complexity and scope of security issues associated with private 5G networks. The targeted selection ensures that the research not only identifies key security concerns but also highlights areas requiring further investigation and development, thus contributing to the advancement of security frameworks within this technological landscape.

To maintain a focus on the most recent advancements and discussions, the review prioritized articles published within the past decade, specifically from 2014 to 2024. This period reflects the latest in private 5G technology and security concerns, aligning with rapid innovation in the field. Given the evolving nature of 5G security, selecting studies within this period ensures that the review captures contemporary research trends and emerging security threats that may not have been previously considered. By adhering to strict inclusion criteria, the review excluded studies lacking empirical evidence, theoretical rigor, or relevance to private 5G security. This methodological approach ensures that the studies included in the review contribute meaningfully to answering the research questions while maintaining high standards of credibility and academic accuracy. Furthermore, the inclusion of diverse perspectives and methodological frameworks across the selected literature enriches the synthesis process, offering a nuanced understanding of the security challenges faced by private 5G networks. This foundation is critical for drawing informed conclusions and identifying potential directions for future research in the field.

4. Methodology

4.1 Systematic Literature Review (SLR)

The SLR methodology serves as the foundation for this research into security vulnerabilities in private 5G networks. The SLR methodology is distinguished by its structured and transparent approach to synthesizing existing knowledge on a specific topic. According to Mengist et al. (2020), the SLR enables researchers to collect and evaluate evidence systematically, ensuring the findings are comprehensive and reproducible. The SLR methodology is executed in distinct stages, beginning with the formulation of clear and focused research questions that guide the entire review process. These questions are instrumental in determining which studies are relevant for inclusion. Following this, a comprehensive search of databases is conducted to identify all available research that meets the predefined inclusion criteria. Once studies are gathered, they undergo a critical appraisal to assess their quality, followed by structured data extraction and synthesis. This multi-step process ensures that only the most relevant, high-quality studies are included, minimizing the potential for bias and enhancing the reliability of the findings.

The SLR is particularly well-suited to research areas that are complex and evolving, such as the security challenges in private 5G networks. Given the rapid pace of technological change and the emergence of new vulnerabilities, an SLR allows for a thorough exploration of existing literature to identify both well-documented issues and less-explored vulnerabilities. By adhering to strict inclusion and exclusion criteria, the methodology ensures the selection of studies that are directly relevant to the research questions, thereby ensuring a high level of precision and relevance in the findings. By using this method, the study ensures that a broad range of peer-reviewed journal articles, conference papers, white papers, and technical reports are considered, allowing for a holistic view of the security landscape of private 5G networks.

4.1.1. Rationale for Using SLR

The choice of employing the SLR methodology in this research is driven by critical factors, rendering it especially appropriate for investigating security vulnerabilities within private 5G networks. As Mengist et al. (2020) note, the SLR offers a robust, replicable framework for synthesizing existing research, making it an ideal choice for addressing the complex and evolving security challenges in this domain. Private 5G networks present unique and intricate security concerns, particularly in areas such as network slicing, edge computing, and software-defined networking (SDN). While these issues are critical to the overall security of 5G networks, the existing literature often lacks comprehensive coverage, and many studies focus on broader 5G security topics without delving into private network-specific vulnerabilities. The SLR methodology, through its systematic and transparent approach, allows for the identification and synthesis of research that specifically addresses these under-explored vulnerabilities. This is crucial for advancing the body of knowledge in a rapidly changing field, as it uncovers gaps where further investigation is necessary.

Furthermore, the SLR process facilitates the identification of emerging trends and areas where the current research is contradictory or outdated. For example, while vulnerabilities in supply chain dependencies and 5G infrastructure have been acknowledged in broader 5G studies, they remain under-researched in the context of private 5G networks. The SLR approach helps identify these areas of neglect, highlighting critical gaps that need attention. Mengist et al. (2020) emphasize that this ability to map out gaps in the literature is one of the key strengths of the SLR, allowing for future-focused research and practical recommendations. In addition to identifying gaps, the SLR ensures that the analysis is objective and consistent. By adhering to predefined inclusion and exclusion criteria, the methodology minimizes bias and ensures that only relevant studies are considered, which enhances

the credibility and reliability of the findings. The structured nature of the SLR also ensures that the results are directly aligned with the research objectives, providing a strong foundation for drawing evidence-based conclusions. Overall, the SLR methodology is well-suited for addressing the unique security challenges of private 5G networks. By synthesizing a broad range of studies and systematically identifying research gaps, the SLR provides a comprehensive understanding of the field and forms the basis for future research and practical recommendations to mitigate vulnerabilities in private 5G deployments.

4.1.2. Overview of the SLR Process

The SLR methodology is typically conducted in a series of distinct stages, each designed to ensure the process is thorough, consistent, and able to be replicated. These stages are structured to provide a complete synthesis of existing knowledge while minimizing subjectivity and ensuring that only the most relevant and high-quality studies are included. The key stages of the SLR process are outlined below. One of the defining aspects of the SLR process is its emphasis on clear and detailed documentation at every stage, which allows others to replicate the review. This emphasis on transparency is a hallmark of the SLR methodology, distinguishing it from other forms of literature review. By adhering to recognized standards such as PRISMA or Cochrane guidelines, the SLR ensures that the process is both dependable and consistent, avoiding any undue influence on study selection or analysis. The initial phase involves the development of focused research questions, which define the scope and objectives of the review. These questions ensure that the review addresses specific issues of interest, such as the security vulnerabilities within private 5G networks, and that the studies included directly contribute to answering these questions.

Following this, the search and selection phase takes place, where relevant studies are gathered from multiple sources. This process includes applying strict inclusion and exclusion criteria to ensure that only studies that meet the necessary academic and methodological standards are considered. By using these criteria, the selection process is refined to focus on studies that are most pertinent to the research, minimizing the risk of introducing irrelevant or biased sources. Once studies are selected, data extraction and synthesis occur, where essential information from each study, such as methodologies, findings, and context are systematically gathered. This data is then organized to allow for comparative analysis, enabling the identification of common themes, discrepancies, and unexplored areas in the literature. The review concludes with a synthesis of the results, where the aggregated data is analysed to draw conclusions about the current state of knowledge and identify areas requiring further investigation. This final step not only summarizes the key findings but also provides guidance for future research directions, helping to address unresolved issues within the field. By following these well-defined stages, the SLR methodology ensures a comprehensive, objective, and high-quality review of the literature, offering valuable insights into the research topic.

4.2. Defining the Research Question

The first and most critical step in conducting a SLR is the formulation of a clear and well-defined research question. This is essential for ensuring that the review remains focused and relevant, guiding the process of selecting studies that directly address the research problem. In this study, the central research question is: What are the key security vulnerabilities in private 5G networks? To ensure that all relevant aspects of this broad topic are covered, the central question is subdivided into specific sub-questions. These sub-questions are designed to address key dimensions of the topic, including:

- What specific vulnerabilities exist within private 5G networks?
- How do these vulnerabilities impact the confidentiality, integrity, and availability of data?

- What mitigation strategies have been proposed to address these vulnerabilities in the literature?

This structured approach of breaking down the central research question into smaller, manageable sub-questions helps narrow the scope of the review while ensuring that all critical facets of the topic are thoroughly examined. By guiding the selection of studies, these questions help ensure that the review comprehensively addresses the security vulnerabilities specific to private 5G networks(Mengist et al., 2020).

4.3. Selecting Databases and Research Sources

A critical component of conducting a thorough and comprehensive SLR is the careful selection of relevant databases and research sources. This process ensures that the review encompasses a wide spectrum of high-quality studies and accurately represents the current state of research on security vulnerabilities in private 5G networks. To achieve a well-rounded analysis, it is essential to source literature from reputable, peer-reviewed databases that specialize in telecommunications, cybersecurity, and engineering disciplines. In this thesis, the following academic databases were selected based on their relevance to the research topic and their ability to provide access to authoritative and up-to-date literature:

- IEEE Xplore: Recognized for its extensive repository of peer-reviewed journal articles and conference proceedings in electrical engineering, computer science, and telecommunications. This database is particularly valuable for accessing innovative research on 5G security.
- ScienceDirect: Offers a broad range of scholarly publications in engineering, computer science, and applied sciences. It is instrumental in identifying key studies on cybersecurity risks and emerging threats in private 5G networks.
- ResearchGate: Provides access to preprints, open-access articles, and research shared by scholars, often capturing studies not indexed in traditional academic databases. It serves as a supplementary resource to track emerging discussions in the field.
- SpringerLink: Contains a diverse collection of authoritative journal articles and conference proceedings, offering insights into theoretical and practical aspects of 5G security vulnerabilities.
- Google Scholar: Used as a supplementary source to broaden the search beyond traditionally indexed databases. It captures grey literature, white papers, dissertations, and technical reports that contribute to a holistic understanding of private 5G security.

By utilizing these databases, this review ensures a comprehensive examination of security vulnerabilities in private 5G networks. The selection of diverse sources allows for a balanced analysis, incorporating both well-established research and emerging insights. This approach minimizes bias, enhances the depth of the literature review, and strengthens the reliability of findings by ensuring that a wide range of perspectives and methodologies are considered.

4.4. Defining Search Terms, Keywords, and Scope

To ensure a thorough and relevant search of the selected databases, a comprehensive search strategy was developed, focusing on keywords aligned with the core research questions of security vulnerabilities in private 5G networks. The search terms were carefully chosen to cover both fundamental security aspects and emerging concerns in private 5G environments.

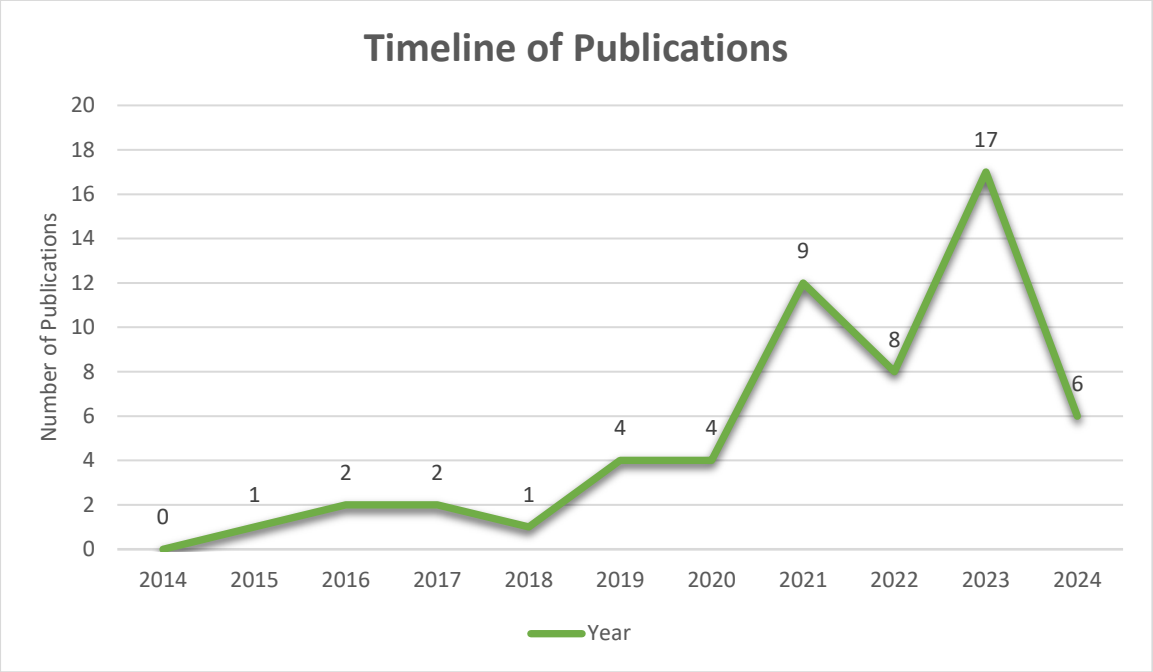
The primary keywords included:

- Private 5G Network
- Non-Public 5G Networks
- Standalone Non-Public Networks
- 5G Network Security Challenges
- Security Vulnerabilities in Private 5G Networks

The scope of this review was carefully defined to ensure relevance to current security challenges in private 5G networks. The study focused on publications from 2014 to 2024, a period marked by significant advancements in 5G technology. Boolean operators and advanced search techniques were employed to refine the search process, capturing both theoretical and practical security solutions. This structured approach provided a strong foundation for analyzing vulnerabilities and mitigation strategies. Figure 2 presents a graphical summary of the selected studies published per year within this timeframe. The distribution reflects the increasing academic and industry focus on private 5G network security, particularly in recent years. The surge in publications in the latter half of the period underscores the growing urgency in addressing security concerns as private 5G deployments expand.

Figure 2

Number of Relevant Studies Published on Security Vulnerabilities in Private 5G Networks.



Note. This data was collected through the number of studies used in this thesis. Own Work.

4.5. Merging Results from Multiple Databases

After executing the search queries across the selected databases, the next step was to consolidate the results into a single, comprehensive collection for further review. This consolidation ensured that studies from various sources were included, minimizing the risk of missing valuable research. By combining results from databases such as Scopus, IEEE Xplore, ScienceDirect, and supplementary sources like Google Scholar, the review captured a broader range of research, encompassing various disciplines and perspectives on the security vulnerabilities of private 5G networks. Merging results from multiple databases also addressed potential biases or gaps that could arise from relying on a single source, especially given differences in indexing practices and database specific limitations. This approach provided a diverse pool of literature, reflecting a wide spectrum of academic work. The final

data collection formed the foundation for identifying trends, patterns, and gaps in the research, ensuring that the SLR process was both exhaustive and provided a comprehensive view of the security challenges faced by private 5G networks.

4.6. Screening, Study Selection, and Eligibility Criteria

The study selection process for this SLR was designed to be structured and rigorous, ensuring that the final set of studies was both relevant and of high academic quality. This multi-stage process was critical for filtering studies based on their alignment with the research objectives and adherence to clearly defined eligibility criteria, which were established to maintain the focus and integrity of the review.

Eligibility Criteria

To ensure that the studies selected were both high-quality and directly relevant to the research topic, the following eligibility criteria were applied:

- Relevance to Research Questions: Only studies that directly addressed security vulnerabilities, risks, and threats within private 5G networks were included. Research focused on public 5G networks or unrelated technologies, such as IoT in non-telecom fields, was excluded. This was essential to maintain the review's focus on the specific security concerns of private 5G networks.
- Recency: To capture the most current advancements, only studies published within the last decade (2014–2024) were prioritized. This exclusion of outdated or irrelevant information was particularly important, given the rapid advancements in 5G technology and the evolving nature of associated security challenges.

These eligibility criteria were essential for ensuring the relevance and academic integrity of the studies selected for inclusion. They served as a foundation for maintaining the reliability of the review and ensuring that the selected studies comprehensively addressed security challenges in private 5G networks. A total of 300 articles were initially identified during the early stages of the SLR, sourced from a range of academic databases and scholarly platforms. The initial distribution was as follows: IEEE with 110 articles, ScienceDirect 25, ResearchGate 60, Google Scholar (including general and miscellaneous articles) accounted for 95, SpringerLink 45, and Scopus with 55 articles.
Following a rigorous exclusion process, which involved filtering out studies not focused on security vulnerabilities in private and public 5G networks, as detailed in this section, the final number of articles included in the SLR was 55. These were selected based on relevance, quality and alignment with the research scope. The final distribution included 24 articles from IEEE, 9 from ScienceDirect, 6 from ResearchGate, 6 from Springer (including 1 from SpringerLink), and 9 from Google Scholar. A comprehensive list of all included articles, along with their titles and authors, is provided in the appendix.

Study Selection Process

The study selection process followed a systematic, multi-stage approach to ensure that only studies meeting the eligibility criteria were included in the final set:

1. Initial Sorting: In the first stage, a list of potentially relevant articles was compiled. Titles and abstracts were initially reviewed to assess alignment with the research topic. Articles that clearly addressed security vulnerabilities in private 5G networks advanced to the next stage.

2. Abstract Review: In the second phase, abstracts were critically assessed for relevance to the research questions. Only those studies that explicitly addressed security risks or challenges in private 5G networks were moved forward. This step ensured that irrelevant studies were filtered out early in the process.

3. Full-Text Evaluation: Studies that passed the initial review were then subjected to a full-text examination. This comprehensive review focused on evaluating the study's methodology, research design, findings, and overall contribution to understanding security vulnerabilities in private 5G networks. Studies that lacked methodological rigor or did not meet the research objectives were excluded at this stage.

4. Final Selection: The final selection comprised studies that met all eligibility criteria and demonstrated a significant contribution to understanding security vulnerabilities in private 5G networks. This multi-stage, rigorous selection process ensured that the final set of studies was both comprehensive and high-quality, laying a solid foundation for subsequent data extraction and synthesis.

Inclusion and Exclusion Criteria

- Inclusion Criteria: Studies were included if they addressed security vulnerabilities, risks, or challenges in private 5G networks, were peer-reviewed, and were published within the last decade.
- Exclusion Criteria: Studies were excluded if they focused on public 5G networks, were not related to private 5G security, came from databases not previously mentioned, or did not meet the standards for academic rigor.

By applying these stringent eligibility criteria, the SLR process ensured that only the most relevant and high-quality studies were included. This careful screening process was essential for synthesizing insights into the security vulnerabilities of private 5G networks and providing a robust foundation for future research.

4.7. Review and Data Extraction Process

The review and data extraction process focused on systematically analysing the selected studies to identify key security vulnerabilities, emerging trends, and mitigation strategies within private 5G networks. This phase ensured that insights were synthesized in a structured manner, facilitating a comprehensive understanding of the research landscape.

Review Methodology

Once studies were selected based on eligibility criteria, an in-depth qualitative assessment was conducted to evaluate their contributions. The selected studies were classified based on their research approach, security focus, and technological relevance. The assessment criteria included:

- Security Domains Covered: Studies were categorized by specific security concerns, such as authentication mechanisms, encryption protocols, intrusion detection, and attack surfaces unique to private 5G networks.

- Methodological Approaches: The research methodologies, whether experimental, simulation-based, theoretical, or case study driven, were examined to assess the depth and validity of findings.

- Industry and Sector Relevance: Studies were further analysed to determine their focus areas, such as industrial automation, healthcare, smart cities, and critical infrastructure, to highlight real-world applicability.
- Innovation and Novelty: Research that introduced new security frameworks, protocols, or mitigation strategies was distinguished from those that reinforced existing knowledge.

This structured classification enabled a clearer understanding of how different studies contributed to the broader security discourse in private 5G networks.

Data Extraction and Thematic Analysis

Following the categorization, a structured data extraction framework was applied to systematically gather relevant information from each study. The extracted data was organized into key themes to ensure consistency and facilitate comparative analysis. The primary extraction elements included:

- Identified Security Risks: Each study's findings on vulnerabilities, such as supply chain threats, AI-driven attacks, or insider threats, were recorded and analysed for commonalities.
- Proposed Mitigation Strategies: Studies that introduced solutions, such as blockchain-based security frameworks, zero-trust architectures, or quantum-safe cryptography, were examined for effectiveness and feasibility.
- Implementation Challenges: Research that discussed deployment barriers, regulatory considerations, and cost implications of security solutions were reviewed to provide a practical perspective on mitigating security risks in private 5G networks.
- Emerging Trends and Research Gaps**:** Key insights on underexplored areas, such as security risks in 6G-prepared private networks, AI-driven threat intelligence, or interoperability challenges, were extracted to highlight future research directions.

By applying this structured review and data extraction approach, the analysis ensured a comprehensive synthesis of security vulnerabilities and mitigation techniques in private 5G networks. The extracted insights were instrumental in shaping the discussion on existing gaps and future directions, reinforcing the study's objective of identifying critical security challenges within this domain.

4.8. Synthesizing the Results

The final stage of the SLR involves the synthesis of findings from the selected studies. This step is critical for integrating the diverse insights gathered throughout the review and translating them into meaningful conclusions. The synthesis process begins with summarizing the key findings of each study, focusing on aspects related to security vulnerabilities in private 5G networks. This includes analysing the types of vulnerabilities identified, the specific threats they pose to network operations, and the mitigation strategies proposed within the literature. A vital component of this synthesis is identifying recurring themes and patterns across the studies. By examining these commonalities, the review highlights areas of agreement among researchers, providing a consolidated understanding of the prevailing security concerns in private 5G networks. Equally important is identifying points of divergence or contention, as these often-signal areas requiring further exploration or debate within the research community.

In addition to identifying consensus and disagreements, the synthesis process plays a crucial role in uncovering research gaps. These gaps represent areas where the existing body of knowledge is either incomplete or insufficient, providing opportunities for future studies to address unresolved issues. For example, gaps may emerge in understanding specific vulnerabilities related to emerging technologies, such as network slicing or edge computing within private 5G environments. The synthesis culminates in a comprehensive overview of the security landscape of private 5G networks, addressing the core aspects of vulnerabilities, threats, and mitigation strategies. This integrated perspective not only informs the answers to the research questions but also underpins the broader conclusions and implications of this study. By systematically combining the insights from individual studies, the synthesis ensures that the findings are both robust and aligned with the objectives of the SLR.

5.Results and Findings

The results and findings of this study are the culmination of a meticulous and systematic review of the existing literature, aimed at uncovering and analysing the security vulnerabilities specific to private 5G networks. This investigation has illuminated the evolving research landscape, highlighting critical vulnerabilities and shedding light on the unique cybersecurity challenges faced by private 5G deployments. By focusing on private 5G networks, which are tailored to meet the specific requirements of enterprises and industries, this study identifies how their architecture, deployment scenarios, and operational environments introduce distinct risks compared to public 5G networks.

Through this review, the analysis not only uncovered significant progress in addressing security challenges but also revealed notable gaps, particularly in the development of tailored frameworks and strategies for private 5G networks. These findings emphasize the need for targeted solutions that go beyond the general measures applied to public 5G networks, accounting for the bespoke configurations, localized deployments, and specialized use cases of private networks. In the subsequent section, this study will delve deeper into a comparative analysis of vulnerabilities between private and public 5G networks, highlighting the unique threats and security considerations that differentiate the two. This comparison is essential for understanding how the distinct nature of private 5G networks shapes their threat landscape and underscores the importance of designing specialized security measures to address their unique requirements.

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

Public and private 5G networks share a foundational architecture but differ significantly in their operational environments, deployment use cases, and security challenges. A review of the existing literature reveals distinct vulnerabilities unique to private 5G networks, while also highlighting overlapping concerns with public 5G deployments. This comparison emphasizes the need for tailored security strategies to address the specific vulnerabilities of private 5G networks.

Authentication and Authorization Flaws

Authentication and authorization are critical challenges in both public and private 5G networks, though their implications vary due to differing deployment contexts. Public 5G networks rely on established protocols, such as 3GPP-defined authentication mechanisms, to manage many users across a shared infrastructure. While these protocols are robust, they are still susceptible to threats like SIM jacking and identity spoofing (Tripathi et al., 2022). In contrast, private 5G networks often face authentication and authorization vulnerabilities due to weak access control policies and insufficient mechanisms tailored to enterprise environments. The lack of granular role-based access control or multi-factor authentication can expose private networks to insider threats and unauthorized access (Alanazi, 2023). This is particularly concerning in private deployments where sensitive operations, such as industrial automation, demand secure and seamless connectivity.

Data Privacy and Integrity Risks

Data privacy and integrity are pressing concerns in both public and private 5G networks. Public networks face risks due to the scale of data transmission across shared infrastructures, which can be vulnerable to threats such as eavesdropping and data tampering. The presence of diverse user groups and integration with public cloud resources further exacerbate these risks (Tripathi et al., 2022). Although private 5G networks are more contained, they are not immune to these issues. Vulnerabilities are heightened when private networks interface with legacy systems or public infrastructure, creating opportunities for attackers to intercept or manipulate data (Tripathi et al.,

2022). The proprietary nature of private 5G networks also adds complexity, as custom implementations may inadvertently introduce untested security flaws.

Network Slicing Vulnerabilities

Network slicing is a feature common to both public and private 5G networks, but it introduces distinct security challenges in each(Ahokangas et al., 2021). In public 5G networks, misconfigurations in network slicing can lead to cross-slice attacks, where insufficient isolation between slices allows malicious actors to compromise multiple services simultaneously (Tripathi et al., 2022). In private 5G environments, network slicing is often employed to segregate critical applications, such as industrial IoT or healthcare systems, from other operational workloads. However, the lack of robust isolation mechanisms or mismanagement of slice configurations can lead to unauthorized access to sensitive data or operations. These vulnerabilities are further amplified by the need for customized slice implementations in private networks, which may introduce inconsistencies and security gaps.

Denial-of-Service (DoS) Attacks

DoS attacks are a shared vulnerability in both public and private 5G networks, though their impacts differ. In public 5G networks, DoS attacks typically target large-scale services, such as mobile internet or VoIP applications, disrupting resources and degrading service availability. These attacks often target the Radio Access Network (RAN) or core network (Corici et al., 2021). In private 5G networks, the consequences of a DoS attack are more severe due to the specialized, mission-critical nature of the applications they support. For example, a DoS attack targeting a private 5G network deployed in an industrial setting could halt production lines or disrupt healthcare operations, leading to significant financial and operational losses (Ahad et al., 2023). The more focused scope of private networks makes them attractive targets for attackers, who can direct their efforts toward specific, high-value assets.

Systemic Challenges in Addressing Vulnerabilities

Both public and private 5G networks face systemic challenges in mitigating security risks. However, private 5G networks are particularly hindered by the lack of mature, standardized security frameworks tailored to their unique environments. While public networks benefit from established protocols and extensive research, private networks often rely on ad hoc security implementations that may lack consistency or robustness (Corici et al., 2021). Moreover, the integration of IoT devices and legacy systems is a common concern in both types of networks, but the impact is more pronounced in private networks due to their specialized nature. These integrations introduce additional entry points for attackers and increase the complexity of securing the network.

Conclusion

While public and private 5G networks share several common vulnerabilities, the unique operational requirements and configurations of private networks create distinct security challenges. The absence of standardized security frameworks, coupled with risks such as misconfigured network slices, weak authentication, and the integration of legacy systems, highlights the need for targeted research and customized security solutions. As private 5G networks continue to expand across various industries, addressing these vulnerabilities will be essential to ensuring their security and reliability. Table 3 outlines the most common vulnerabilities in private 5G networks, highlighting the challenges they pose to organizations and their impacts on network security, functionality, and reliability. This summary serves as a valuable resource for identifying key areas of focus to mitigate risks and emphasizes the connection between technical vulnerabilities, operational challenges, and overall network performance. It provides a framework for stakeholders to prioritize efforts in enhancing the security of private 5G networks.

Table 3

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
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.

5.2. Analysis of Findings

The SLR provided a comprehensive examination of the security vulnerabilities integral to private 5G networks. The findings reveal a wide array of challenges that highlight the multifaceted nature of securing these advanced networks(Chin et al., 2023). The reviewed studies pointed to several key areas of concern, emphasizing both technical and operational vulnerabilities that require immediate and collaborative action from stakeholders, including equipment vendors, network operators, service providers, and regulatory authorities. A recurring theme across the literature is the complexity of private 5G networks, which are characterized by their highly customized architectures and varied deployment scenarios. This complexity introduces unique security challenges that distinguish private 5G environments from their public counterparts. For example, issues related to authentication mechanisms and access control policies were frequently identified as critical weaknesses. Inadequate authentication methods can leave networks vulnerable to unauthorized access, a significant risk given the sensitive and mission-critical nature of many private 5G deployments(Alanazi, 2023).

Identified Security Vulnerabilities

Among the most significant security concerns identified were those related to distributed denial of service (DDoS) attacks. These attacks pose a substantial threat to the reliability and availability of private 5G networks, particularly when deployed in industrial or enterprise contexts where operational continuity is paramount. The reviewed studies consistently highlighted the potential for these attacks to disrupt operations, degrade performance, and compromise network reliability. Another area of concern revolves around network slicing vulnerabilities. While network slicing is a powerful feature of 5G technology, allowing multiple virtual networks to operate on the same physical infrastructure, it also introduces risks related to insufficient isolation between slices. Misconfigurations or vulnerabilities in one slice can lead to cascading effects, potentially compromising the entire network. This is particularly relevant for private 5G networks, where slices may be tailored to specific enterprise functions or applications, increasing their exposure to targeted attacks. The studies also emphasized weaknesses in encryption protocols and key management strategies, which are critical for ensuring data confidentiality and integrity. The rapid proliferation of devices within private 5G ecosystems, including IoT devices, further compounds this issue. Many of these devices lack robust security features, creating additional entry points for attackers to exploit.

DDoS Attacks:

Distributed Denial-of-Service (DDoS) attacks are among the most critical threats to private 5G networks due to their potential to overwhelm network resources and disrupt essential services (Ji et al., 2024). These attacks exploit the inherent scalability, low latency, and high throughput capabilities of 5G, leveraging these strengths to

launch large-scale, high-volume attacks. Private 5G networks, often deployed to support critical applications such as industrial automation, smart healthcare, and emergency services, are particularly vulnerable because their downtime can result in significant operational, safety, and financial consequences (Aijaz, 2020). One of the primary challenges posed by DDoS attacks in 5G networks is the growing sophistication of attack methods (Corici et al., 2021). Modern attackers increasingly utilize botnets, large networks of compromised IoT devices to generate massive traffic volumes (Ji et al., 2024). With the proliferation of IoT devices connected to private 5G networks, attackers gain access to a broader attack surface, significantly increasing the scale and impact of these threats. This makes private 5G networks especially vulnerable, as the integration of IoT devices often lacks sufficient security hardening, leaving them susceptible to compromise(Alanazi, 2023). Additionally, the multi-layered architecture of 5G networks introduces multiple points of vulnerability. For example, attackers may target the Radio Access Network (RAN) by exploiting signalling mechanisms or launching attacks on control channels, effectively disrupting communications between devices and the network (Ji et al., 2024). Similarly, attacks on the core network can paralyze critical functions such as network slicing, which isolates resources for specific applications. These disruptions can cascade across interconnected systems, amplifying the overall impact of the attack. Furthermore, the reliance on cloud-based services to support network functions introduces an additional layer of risk, as cloud platforms can become targets for volumetric DDoS attacks that overwhelm service availability(Ahmad et al., 2017).

Spoofing:

Spoofing is a critical security vulnerability in 5G networks that allows attackers to intercept and manipulate legitimate interactions by forging identities or signals. This type of attack typically involves impersonating legitimate users, devices, or network components to gain unauthorized access to the network. By injecting false signals, credentials, or communications, attackers exploit the inherent trust within network authentication protocols (Angin et al., 2022). The implications of such an attack are far-reaching, as spoofing often acts as a precursor to more sophisticated and damaging attacks, including man-in-the-middle (MITM) and denial-of-service (DoS) attacks. For example, in MITM attacks, the attacker intercepts and potentially modifies communications between two legitimate entities, undermining data confidentiality and integrity. In DoS attacks, spoofed requests can overwhelm network resources, rendering them unavailable to authorized users. These critical risks are particularly prominent in private 5G networks due to their reliance on wireless communication, which introduces vulnerabilities at the physical layer of the network(Ahad et al., 2023). The technical complexity of 5G networks further amplifies the risk of spoofing. Advanced technologies such as massive MIMO (Multiple Input Multiple Output) and beamforming, which are designed to enhance performance, coverage, and efficiency, may inadvertently create opportunities for attackers. For instance, imperfections in signal propagation or channel estimation can be exploited by malicious actors to forge signals or masquerade as legitimate devices. Additionally, network slicing, a key feature of 5G, could be targeted to compromise the isolation of network segments, allowing spoofed access to sensitive services or resources(Ahad et al., 2023).

Spoofing attacks also present significant challenges across various applications of 5G technology. In industrial automation environments, a spoofed device could disrupt critical processes by issuing false commands, altering operational parameters, or triggering unauthorized actions, potentially causing financial and operational losses. Similarly, in smart healthcare systems, spoofing could compromise the integrity and confidentiality of sensitive medical data or even enable unauthorized control over connected devices such as patient monitoring systems or infusion pumps. The potential consequences of such breaches are severe, ranging from loss of trust in the system to life-threatening scenarios(Ahad et al., 2023). Given the pervasive and high-stakes nature of spoofing attacks, addressing these vulnerabilities is paramount for securing private 5G networks. Comprehensive security strategies are needed, including the implementation of robust authentication protocols, enhanced encryption methods, and continuous monitoring systems capable of detecting and mitigating spoofing attempts in real time. These measures must be accompanied by ongoing research and innovation to ensure that emerging threats are effectively countered as 5G networks evolve. The risks associated with spoofing highlight the critical importance of a proactive and multi-layered approach to network security(Alanazi, 2023).

Unauthorized Access:

Unauthorized access refers to the act of entering a computer system, network, or data resource without proper authorization. It often involves bypassing established security measures, such as authentication protocols, encryption, or access control mechanisms, to exploit information, applications, or services that are restricted to authorized users. This breach of privacy and security can have serious implications, including data theft, system tampering, unauthorized configuration changes, or serving as a gateway for launching further cyberattacks. Unauthorized access is one of the most critical vulnerabilities highlighted in private 5G networks due to the sensitive and high-value nature of the data they handle(Djuitcheu et al., 2023). Private 5G networks, designed for tailored use in industries such as healthcare, manufacturing, and critical infrastructure, are particularly vulnerable to unauthorized access because they often integrate diverse devices, users, and services. Weak authentication protocols and insufficient access control mechanisms are frequently cited as contributing factors that increase the risk of unauthorized access. For example, the failure to implement multi-factor authentication (MFA) or to regularly update credentials creates exploitable entry points for attackers (Angin et al., 2022). A notable dimension of unauthorized access in private 5G networks arises from supply-chain-related vulnerabilities. During system upgrades, maintenance, or the deployment of new services, malicious actors can infiltrate through compromised software or hardware. For instance, during a routine update, malicious software or firmware could be installed, providing attackers with covert access to network resources. Similarly, tampered hardware devices introduced into the supply chain can function as backdoors, granting attackers persistent unauthorized access to the system. This highlights the need for rigorous supply chain security protocols, including stringent vetting of third-party vendors, thorough inspections of hardware, and cryptographic verification of software updates(Ji et al., 2024).

Jamming:

Jamming attacks pose a significant threat to the integrity and reliability of 5G networks by deliberately interfering with wireless communication. These attacks are executed by overwhelming the network with excessive noise or malicious signals, thereby disrupting the normal transmission and reception of data(Ahad et al., 2023). The primary objective of a jamming attack is to degrade or completely block legitimate communication, which can lead to severe consequences such as service disruptions, data loss, or even full-scale network failures. These attacks are particularly effective against wireless networks due to their reliance on specific frequencies or channels for seamless communication. By targeting these frequencies, attackers can exploit the inherent vulnerabilities of wireless systems, significantly impacting their functionality. In the context of 5G-based smart healthcare networks, jamming attacks present a heightened risk because of the critical role that wireless communication plays in the operation of these systems. Control channels, which are essential for managing the radio interface, are particularly vulnerable to such attacks. An attacker with high-powered signals can target these control channels, causing disruptions that interfere with the frequency bands and compromise the reliability of healthcare services. Moreover, the threat of jamming attacks is exacerbated when multiple devices are compromised and converted into a botnet. In this scenario, hijacked mobile medical devices collectively function as jamming tools, increasing the intensity and scale of the attack. This type of coordinated jamming can severely undermine the performance and dependability of 5G networks, particularly in high-stakes environments like healthcare, where consistent communication is vital for patient care(Corici et al., 2021).

MITM (Man-In-The-Middle) Attacks:

A Man-in-the-Middle (MITM) relay attack is a sophisticated exploit in which an adversary establishes a deceptive communication channel between legitimate entities in a network (Corici et al., 2021). This is achieved through the deployment of counterfeit components such as a fake eNodeB and a fake User Equipment (UE). These entities may be linked locally or remotely via alternative communication technologies. The fraudulent eNodeB entices the victim UE to connect to it under the pretence of being a legitimate network node, while the counterfeit UE mimics a genuine UE when interacting with the network core. This setup enables the attacker to intercept, relay, and manipulate communications between the victim UE and the genuine eNodeB(Lambros Sarakis et al., 2021). Through this mechanism, attackers can inject, modify, or suppress information, potentially leading to compromised confidentiality, integrity, and availability of the network. Beyond relay attacks, MITM encompasses a variety of tactics, each with unique methodologies and consequences. These diverse methods underscore the adaptive nature of MITM attacks, posing a significant threat to network security. The referenced work by Wani, et al.,(2024) , supports the classification of these variations within the MITM framework.

Eavesdropping and Privacy Leaks:

Eavesdropping refers to the act of covertly intercepting or monitoring communications between two parties without their consent, often with the aim of accessing sensitive or confidential information(Ahad et al., 2023). This malicious activity typically involves capturing data transmitted over networks, such as emails, voice calls, or messages,

and analysing it for unauthorized purposes. Such breaches compromise the privacy and security of individuals and organizations, often resulting in serious consequences, including identity theft, financial losses, and reputational damage. Eavesdropping is strongly associated with privacy leaks, which occur when sensitive or personal information is exposed to unauthorized entities. These leaks may arise due to poor data management practices, exploitation of security vulnerabilities, or deliberate breaches, potentially causing significant harm to the affected individuals or organizations. The prevalence of eavesdropping and privacy leaks underscores the critical need for robust data protection measures and secure communication protocols(Lin et al., 2023). Eavesdropping attacks involve an attacker intercepting, modifying, or deleting data in transit between two devices. Such attacks are initiated using various sophisticated techniques and specialized eavesdropping devices designed to monitor conversations and analyse network activities. For instance, attackers with a valid security context can impersonate legitimate network entities, creating a malicious network to eavesdrop on user traffic. This scenario often requires the attacker to be in close physical proximity to the victim to ensure the victim connects to the compromised network. The proximity enables the attacker to maintain access and control over the established malicious connection(Cui et al., 2024).

Authentication Issues:

Authentication issues encompass challenges or vulnerabilities in verifying the identities of users, devices, or systems before granting access to resources or services. These vulnerabilities can significantly compromise the security of a system when exploited by attackers. Key concerns in this area include weak password practices, flaws in biometric systems, and inadequate implementation of multi-factor authentication (MFA). Insecure password practices, such as using easily guessable passwords, reusing credentials across multiple accounts, or failing to enforce strong password policies, represent a critical vulnerability (Suraci; et al., 2021). These weaknesses allow attackers to employ brute force or credential-stuffing techniques to compromise accounts(Ahad et al., 2023). Flaws in biometric systems present another significant issue. Although biometric authentication methods, like fingerprint or facial recognition, are considered advanced, they are not immune to exploitation(Alwahaishi & Zdrálek, 2020). The improper implementation of MFA also poses a considerable risk. While MFA strengthens security by requiring multiple verification factors, weaknesses such as reliance on SMS-based authentication can expose systems to interception or SIM-swapping attacks(Djuitcheu et al., 2023). Additionally, authentication mechanisms that fail to assess contextual factors, such as access attempts based on location, device, or behavioural patterns may inadvertently grant unauthorized access (Alanazi, 2023). Authentication vulnerabilities have severe consequences. Exploited weaknesses can lead to unauthorized access to sensitive data, account compromises, or infiltration of secure systems. Such breaches may result in financial losses, operational disruptions, or reputational damage for affected organizations (Alanazi, 2023).

Fake Base Station Attacks

Fake Base Stations (FBS), also known as Rogue Base Stations (RBS), present a significant threat to 5G networks, especially in environments where automation is used for network optimization and management (Ahad et al., 2023). These rogue

stations impersonate legitimate base stations by broadcasting system information at higher signal strengths, tricking user equipment (UE) into connecting to them (Ahad et al., 2023). Once connected, attackers can intercept, manipulate, or exploit user communications, leading to privacy breaches, credential theft, and denial-of-service attacks. The exploitation of FBS typically follows a structured sequence. Initially, attackers passively monitor public broadcast signals to extract network configuration parameters. With this information, they configure an FBS to mimic a legitimate network. Once the rogue station is deployed, it can execute two primary types of attacks: unicast message attacks, which target specific users by intercepting and modifying their communication streams, and paging message attacks, which disrupt network paging messages, causing missed calls, delayed notifications, or message interception. A particularly concerning threat associated with FBS is IMSI-catching attacks, where the rogue station tricks devices into revealing their International Mobile Subscriber Identity (IMSI), a unique identifier for each subscriber's device (Ahmad et al., 2017). Attackers can then use this information to track individuals, compromise network security, or conduct additional targeted attacks. Furthermore, FBS attacks can lead to location-based privacy breaches through techniques like semantic information attacks, timing attacks, and boundary attacks, which allow attackers to infer subscriber locations based on network behaviour (Ahmad et al., 2017). The risks associated with FBS attacks are amplified by vulnerabilities in access point selection algorithms, making it easier for attackers to manipulate UE connection decisions.

Fake User Equipment

Fake User Equipment (UE) refers to malicious devices designed to mimic legitimate UEs within a network(Wani et al., 2024). By using Software-Defined Radios (SDRs) and software-based UE modem implementations, attackers can bypass authentication mechanisms, intercept sensitive communications, and disrupt network operations (Cui et al., 2024). These threats are especially concerning in private 5G networks, where maintaining strong authentication and access control is vital for security. Fake UEs typically exploit authentication weaknesses and human behaviour to gain unauthorized access. Common attack methods include identity spoofing, where attackers impersonate legitimate devices to bypass security checks; phishing attacks, where users are deceived into downloading malicious applications or providing credentials, granting attackers access to the network(Suraci; et al., 2021) and malware deployment, where once access is gained, attackers install malware to maintain persistence, exfiltrate data, or disrupt critical operations. In addition to external exploits, insider threats significantly contribute to fake UE attacks. Malicious insiders may deliberately install rogue devices or grant unauthorized access, undermining security from within (Tripathi et al., 2022). This is particularly dangerous in private 5G networks, where security often depends on controlled environments. Attackers can also manipulate user behaviour, using social engineering tactics to trick employees into connecting to rogue networks or sharing sensitive credentials(Alanazi, 2023). The consequences of fake UE attacks go beyond unauthorized access. By mimicking legitimate devices, attackers can intercept sensitive communications, disrupt authentication processes, and manipulate network resource allocation (Alanazi, 2023). This is particularly concerning in networks utilizing network slicing, where attackers can target specific slices dedicated to critical applications, potentially leading

to service disruptions and security breaches (Wani et al., 2024). Even in highly secure private 5G environments with strong supply chain protections, the UE remains a primary attack vector, often exploited through compromised user behaviour and software vulnerabilities (Tripathi et al., 2022).

Broader Implications and Challenges

Regulatory and governance challenges were another common thread identified in the reviewed literature. The absence of standardized security frameworks tailored specifically for private 5G networks leads to inconsistent security implementations, increasing the risk of vulnerabilities(Wani et al., 2024). Unlike public 5G deployments, which follow stricter regulatory oversight, private 5G networks vary in their security postures, depending on regional policies and organizational practices (Wen et al., 2022). This underscores the urgent need for unified security guidelines that address the distinct requirements of private 5G deployments, including localized infrastructure and compliance requirements across industries (Wen et al., 2022). The findings also highlight the critical role of collaborative efforts among technology providers, network operators, and regulatory bodies. Effective security measures require coordinated action to establish robust standards and best practices (Corici et al., 2021). Studies emphasize the importance of partnerships and shared intelligence in mitigating risks and enhancing the security posture of private 5G networks (Aijaz, 2020). The exchange of threat intelligence, joint security initiatives, and interoperability standards are essential for strengthening overall network resilience (Alanazi, 2023).

Contextual Insights

While the SLR identified numerous vulnerabilities in private 5G networks, it also highlighted gaps in research. Notably, few studies have conducted comparative security analyses between private 5G networks and legacy systems like Wi-Fi or public 5G(Tripathi et al., 2022). Understanding these distinctions would provide valuable insights into the unique challenges of securing private 5G deployments. Additionally, while advanced threat modelling techniques such as attack graphs are widely used in cybersecurity, their application in private 5G network security remains underexplored. Employing structured methodologies to assess vulnerabilities could enhance risk mitigation strategies and contribute to the development of more resilient private 5G security frameworks. In summary, the findings of this SLR underscore the evolving threat landscape of private 5G networks. From authentication weaknesses and encryption flaws to DoS risks and regulatory gaps, addressing these challenges requires targeted research, robust security frameworks, and collaborative efforts. Strengthening security measures will be essential for ensuring the successful and secure deployment of private 5G networks across critical sectors.

5.2.1. Themes and Patterns

From the synthesis of the reviewed literature, several significant themes and patterns emerged, providing critical insights into the key challenges and opportunities within the domain of private 5G networks.

Regulatory and deployment challenges: One major theme involves the regulatory and deployment challenges faced by organizations aiming to adopt local and private 5G networks. Ahokangas et al. (2021) highlighted significant regulatory hurdles, particularly around extended timeframes for spectrum allocation. Such delays can impede timely network implementation, ultimately stalling technological advancements (Frank et al., 2022). Another considerable challenge identified is the limited availability of affordable spectrum, which presents a barrier, especially for smaller enterprises seeking to deploy private 5G solutions (Ahokangas et al., 2021). The complexity and cost of the

authorization process further exacerbate these challenges, leading to financial and logistical burdens(Ahokangas et al., 2021). These regulatory obstacles emerged as a recurring theme across the literature, emphasizing their critical role in shaping both the deployment and security landscape of private 5G networks(Eswaran & Honnavalli, 2023). Given these issues, the findings strongly suggest the need for streamlined regulatory frameworks and more accessible spectrum allocation processes. Such measures would not only facilitate the efficient deployment of private 5G technologies but also contribute to their secure adoption across industries.

Authentication and Access Control: Another recurring theme in the literature is the critical importance of robust authentication mechanisms in safeguarding private 5G networks(Ahad et al., 2023). Authentication vulnerabilities, if left unaddressed, can result in significant security breaches that compromise the confidentiality and integrity of data transmitted over these networks. One key challenge highlighted across several studies is the need to maintain non-repudiation, ensuring that actions taken within the network can be reliably traced back to specific users or entities. This is essential for preventing unauthorized access and misuse, which could otherwise undermine network security. To address these challenges, innovative solutions are being explored. One such solution is Software-Defined Perimeter (SDP) technology, as proposed by Kim et al. (2023). SDP offers a secure architecture for private 5G networks by establishing a perimeter around sensitive resources, ensuring that only authenticated and authorized users or devices are allowed access. By creating a zero-trust model, where access is granted based on identity and not location, SDP significantly reduces the risk of unauthorized network infiltration. This approach is seen as a promising solution to mitigate the authentication and access control issues commonly identified in 5G networks, providing an additional layer of security to prevent threats such as unauthorized data interception and network breaches. Furthermore, the adoption of multi-factor authentication (MFA) and device authentication protocols has been suggested as supplementary measures to strengthen network defences(Lin et al., 2023). These technologies ensure that only verified users and devices can interact with the network, making it more resilient against unauthorized access and malicious actors.

Network Slicing and Isolation Risks: Network slicing is a fundamental feature of 5G networks that allows for the partitioning of network resources to cater to different applications and use cases. While this approach offers significant benefits in terms of resource allocation and efficient management, it also introduces several security risks that can compromise the integrity of private 5G networks. Studies by Djuitcheu et al. (2023) and V et al. (2022) have highlighted key vulnerabilities associated with network slicing, particularly in relation to the potential for slice isolation bypass and traffic manipulation. In the context of private 5G networks, network slicing is often employed to create isolated virtual networks for different types of traffic, such as enterprise communications, IoT devices, and critical infrastructure. This separation ensures optimal resource usage and performance for each type of traffic. However, when slice isolation is not properly implemented or maintained, attackers can exploit weaknesses to gain unauthorized access to sensitive network slices. This breach of isolation can result in cross-slice contamination, where malicious actors manipulate or intercept traffic from other slices, potentially leading to data leakage, service disruptions, or even denial-of-service (DoS) attacks.

The risk of traffic manipulation is another significant concern. Malicious users or attackers may exploit vulnerabilities in the slicing mechanism to alter the flow of traffic between slices, resulting in redirection of sensitive data, unauthorized access to network resources, or degradation of service quality across the network. Djuitcheu et al. (2023) emphasized that without effective safeguards, such as advanced encryption, strict authentication protocols, and secure slicing mechanisms the security of slices in private 5G networks remains highly vulnerable. Similarly, V et al. (2022) pointed to the need

for continuous monitoring and robust isolation techniques to ensure that the security of one slice does not compromise the others, particularly when dealing with mission-critical applications requiring high levels of trust and confidentiality. Given these risks, it is crucial for private 5G networks to implement comprehensive security measures to prevent isolation bypass and protect against traffic manipulation. Effective solutions include leveraging AI-driven monitoring tools, anomaly detection systems, and intrusion prevention systems (IPS) to maintain robust slice isolation and protect sensitive data from malicious actors.

Diverse Attack Vectors: The reviewed studies identified a wide range of attack vectors that pose significant threats to private 5G networks, affecting their integrity, confidentiality, and availability. One particularly concerning attack is fake base stations, as discussed by Liu et al. (2023). Also known as spoofing attacks, this method involves adversaries deploying unauthorized base stations that masquerade as legitimate ones. By doing so, attackers can intercept user communications, steal sensitive data, or manipulate network traffic. This threat is especially critical in private 5G environments, where sensitive enterprise data is at risk of unauthorized access and interception. Beyond fake base stations, private 5G networks face other sophisticated threats. Angin et al. (2022) identified several key attack vectors, including Denial of Service (DoS) attacks, spoofing, eavesdropping, and tampering. DoS attacks aim to overwhelm network resources by flooding them with excessive traffic, rendering services inaccessible to legitimate users. These attacks are particularly disruptive in private 5G deployments, where network downtime can significantly impact business operations. Similarly, spoofing, and eavesdropping pose serious security risks, allowing attackers to impersonate legitimate network entities or intercept communications, potentially leading to data theft or injection of malicious payloads. Additionally, tampering attacks, which involve altering transmitted data, can compromise communication integrity and introduce security breaches, such as malware propagation.

In their taxonomy of 5G threats, Wani et al. (2024)categorized attacks into active and passive threats, further emphasizing the complexity of securing private 5G networks. Active attacks, such as radio jamming and signal overshadowing, intentionally disrupt wireless communications by injecting interference into the radio frequency spectrum. These attacks can degrade network performance, cause service outages, or prevent devices from maintaining connectivity. On the other hand, passive attacks, such as International Mobile Subscriber Identity (IMSI) leaks, enable attackers to track users or intercept signalling data by exploiting protocol vulnerabilities. IMSI-catching remains a major privacy concern, as it allows adversaries to monitor user locations and potentially conduct further targeted attacks. The diversity of attack vectors outlined in these studies underscores the growing complexity of securing private 5G networks. As these networks evolve and integrate more advanced technologies, both traditional and emerging cyber threats will continue to pose significant risks. Addressing these vulnerabilities requires a multi-layered security approach, incorporating strong encryption, adaptive authentication mechanisms, intrusion detection systems, and continuous network monitoring to mitigate evolving attack methods.

5.2.2. Comparison and Contrast

Comparing and contrasting the findings of different studies reveals several similarities and differences:

5.2.2.1 Similarities

Common Threats: The reviewed studies consistently highlight critical security threats affecting private 5G networks, emphasizing areas where vulnerabilities are particularly pronounced. Among these, Distributed Denial-of-Service (DDoS) attacks emerge as a significant concern due to their ability to overwhelm network resources and disrupt critical services (Ahad et al., 2023; Djuitcheu et al., 2023;

Wani et al., 2024). These attacks exploit the increased connectivity and bandwidth of private 5G networks, making them a high-priority risk. Spoofing attacks, where attackers impersonate legitimate network entities, also pose severe risks. Research highlights how fake base stations can intercept communications, steal data, or manipulate network traffic (Angin et al., 2022; Liu et al., 2023). This underscores the importance of robust authentication mechanisms to prevent unauthorized access. Authentication and access control vulnerabilities are another widely recognized issue. Studies indicate that weak authentication frameworks leave networks susceptible to breaches (Ahad et al., 2023; Kim et al., 2023). In private 5G environments, where multiple devices and users interact, scalable and secure authentication methods are essential.

Additionally, eavesdropping and data tampering are noted as significant risks, particularly when encryption protocols are weak (Angin et al., 2022). Attackers can intercept sensitive data or alter transmissions, compromising network integrity. Network slicing risks, such as slice isolation bypass and traffic manipulation, are also commonly discussed (Djuitcheu et al., 2023; V et al., 2022). Without strong isolation mechanisms, attackers could exploit vulnerabilities in one slice to impact others, undermining security across the entire network. Finally, radio-layer vulnerabilities remain a critical challenge. Active attacks like radio jamming and signal overshadowing degrade network performance, while passive threats such as IMSI leaks compromise user privacy(Wani et al., 2024). These threats emphasize the need for strong physical-layer security protections(Ahad et al., 2023). Overall, the convergence of findings across multiple studies highlights the multifaceted nature of threats to private 5G networks. Addressing shared concerns, such as DDoS attacks, spoofing, weak authentication, and network slicing vulnerabilities, requires a coordinated, multi-layered security approach.

Need for Improved Security Measures: Several studies emphasize the urgent need for security measures tailored specifically to private 5G networks. Unlike public 5G deployments, private networks have distinct operational environments and require customized security solutions (Ahad et al., 2023; Kim et al., 2023). One key area of concern is authentication security. Research suggests that traditional authentication mechanisms are inadequate for protecting sensitive applications, such as smart healthcare and industrial IoT (Ahad et al., 2023). Weak authentication can lead to breaches of confidentiality, integrity, and non-repudiation, highlighting the need for dynamic and context-aware authentication frameworks. A proposed solution to these vulnerabilities is the Software-Defined Perimeter (SDP) model, which strengthens access control through direct trust-based authentication (Kim et al., 2023). SDP enforces strict authentication policies, effectively mitigating risks of unauthorized access and data breaches(Altaleb & Zoltán, 2023).

Another recurring theme is the need for standardized security frameworks. Existing security models are often inherited from public 5G networks or legacy systems and fail to address the unique challenges of private deployments(Kim et al., 2023). Key gaps include:

- Network slicing security: Ensuring complete isolation between slices to prevent unauthorized lateral movement.
- Zero-trust architectures: Applying strict verification policies for all devices and users(Angin et al., 2022).
- Advanced cryptographic mechanisms: Protecting data transmission with quantum-resistant encryption.

The reviewed literature also underscores the importance of collaboration among network operators, device manufacturers, and regulatory bodies. Standardized best practices, shared threat intelligence, and cross-industry cooperation are essential for building resilient private 5G ecosystems. In summary, the consensus across these studies reflects the urgent need for initiative-taking security strategies. By

integrating stronger authentication methods, secure network slicing, and standardized security architectures, private 5G networks can effectively mitigate evolving cyber threats and maintain high security and reliability standards.

5.2.2.2 Differences

Proposed Solutions: The reviewed studies propose diverse approaches to mitigating security vulnerabilities in private 5G networks. These variations highlight the complexity and layer nature of securing these advanced systems, demonstrating that no single solution can comprehensively address all security challenges. One significant distinction in the literature is the architectural approach to network security. Kim et al. (2023) propose a Software-Defined Perimeter (SDP) framework to enhance authentication and access control. The SDP model isolates network resources and enforces strict authentication protocols, mitigating risks associated with unauthorized access, lateral movement, and data breaches. This holistic, system-wide approach targets fundamental weaknesses in traditional access control mechanisms, establishing a secure foundation for private 5G deployments. In contrast, other studies focus on specific threat vectors. Liu et al. (2023) concentrate on the growing threat of fake base stations, which attackers use for spoofing, eavesdropping, and network manipulation. Their research advocates for real-time detection algorithms and network monitoring tools to identify and neutralize these threats. Unlike Kim et al.'s (2023) broad architectural solution, Liu et al. (2023) emphasize specialized, targeted countermeasures that address the operational and technical aspects of a single attack type.

This divergence in approaches underscores the importance of a layered and integrated security strategy. While Kim et al. (2023) advocate for preventive security through robust network architecture, Liu et al. (2023) propose reactive security measures to counter specific attack vectors. Both approaches have merit, but their effectiveness depends on the specific threat landscape and deployment context. Beyond these two perspectives, other studies propose alternative security models, such as:

- Artificial Intelligence (AI)-based threat detection: Leveraging AI and machine learning to identify anomalous behaviour in real time(Alanazi, 2023).
- Blockchain for decentralized security: Enhancing trust and data integrity through distributed ledger technology (Ramezanpour et al., 2023).
- Zero-Trust Network Access (ZTNA): Implementing continuous verification mechanisms beyond traditional perimeter-based security(Altaleb & Zoltán, 2023).

The diversity of proposed solutions indicates that security for private 5G networks cannot rely on a one-size-fits-all approach. Instead, an adaptive and scalable security framework is necessary to address evolving threats. Combining architectural innovations like SDP with targeted countermeasures against specific threats will enhance the overall security posture of private 5G networks. Additionally, the differences in security methodologies suggest the need for continued research. Future studies should focus on:

- Hybrid approaches that integrate architectural frameworks with real-time threat detection(Angin et al., 2022)
- Scalability and performance trade-offs between different security models(Tripathi et al., 2022)
- Standardization efforts to unify diverse security solutions into cohesive frameworks(Ficzere et al., 2021)

Through these varied perspectives, the literature reinforces the necessity of multi-faceted and context-specific strategies. As private 5G networks evolve, a collaborative effort between researchers, industry stakeholders, and regulatory bodies will be crucial to developing robust, future-proof security solutions.

Focus Areas: The reviewed studies highlight a wide spectrum of focus areas, reflecting the diverse contexts in which private 5G network security is examined. These contexts encompass both sector-specific applications and broader, cross-industry perspectives, underscoring the multifaceted nature of private 5G networks and their associated vulnerabilities. One key area of focus is sector-specific security concerns, which address the unique vulnerabilities and requirements of different industries utilizing private 5G networks. Ahad et al. (2023) examine the application of private 5G networks in smart healthcare, where security challenges such as authentication vulnerabilities, confidentiality breaches, and non-repudiation issues pose significant risks. Given the sensitivity of healthcare data and the real-time communication requirements in medical applications, robust security measures are imperative. The study emphasizes tailored security solutions designed to meet the unique operational requirements and regulatory frameworks of healthcare systems, demonstrating the importance of industry-specific security strategies(Djuitcheu et al., 2023).

In contrast, other studies adopt a broader, cross-industry approach. V et al. (2022) and Angin et al. (2022) explore general security risks across multiple private 5G use cases. V et al. (2022) focus on overarching security challenges, including network slicing vulnerabilities and isolation bypass risks, which are relevant across various industries, from industrial automation to enterprise communications. Similarly, Angin et al. (2022) provide a detailed taxonomy of threats, identifying denial-of-service (DoS) attacks, eavesdropping, spoofing, and tampering as key concerns. These studies offer a holistic perspective, helping to identify common security risks that transcend specific industries(Prados-Garzon et al., 2021).

The variation in focus areas underscores the complexity of private 5G network security. While sector-specific analyses provide tailored security solutions to address unique industry needs, broader studies highlight common vulnerabilities that cut across multiple applications. This contrast reinforces the need for adaptable security frameworks that can balance specificity with flexibility, ensuring robust protection for private 5G networks across different environments. To provide a consolidated view of these security threats, Table 4 summarizes the key vulnerabilities identified across the literature. Each threat is accompanied by a brief description, offering a structured reference for understanding the scope and nature of risks in private 5G networks. This table serves as a valuable resource for stakeholders, helping to prioritise security measures and develop more effective mitigation strategies.

Table 4

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 & Traffic Manipulation	Attackers exploit vulnerabilities in one slice to affect others, undermining overall network security.
Radio-Layer Vulnerabilities	Active Threats: Radio Jamming & Signal Overshadowing	Degrade network performance by interfering with wireless signals.
	Passive Threats: IMSI Leaks	Compromise user privacy by exposing unique subscriber identifiers.

Note. This was adapted from various literature as stated in section 5.2.2.1 under similarities, common threats. All authors cited under the same section.

5.2.5. Summary of Findings

The findings from the SLR highlight a range of security vulnerabilities and challenges unique to private 5G networks. Several key themes emerged across the reviewed studies, with a consistent focus on the complexities of securing these networks amidst evolving threats:

1. **Regulatory and Deployment Challenges**: The deployment of private 5G networks is significantly impacted by regulatory barriers, including extended periods for spectrum allocation and limited access to affordable spectrum. These challenges create logistical and financial constraints, hindering the widespread adoption of private 5G technologies. This underscores the need for more streamlined regulatory processes to facilitate efficient deployment.

2. **Authentication and Access Control**: Robust authentication mechanisms are essential to securing private 5G networks. Vulnerabilities in existing authentication systems, particularly in those handling sensitive data, present significant security risks. Solutions such as Software-Defined Perimeter (SDP) architecture have been proposed to address these weaknesses by ensuring secure, trust-based access, thereby enhancing overall network security.

3. **Network Slicing and Isolation Risks**: While network slicing offers critical benefits for resource allocation and traffic management, improper isolation between network slices can lead to severe risks, such as cross-slice contamination and unauthorized data manipulation. To

mitigate these risks, studies emphasize the need for advanced encryption, strict isolation protocols, and continuous monitoring.

4. **Diverse Attack Vectors**: A wide array of attack vectors was identified, including spoofing, fake base station attacks, denial-of-service (DoS) attacks, and eavesdropping. These vulnerabilities can compromise the integrity, availability, and confidentiality of data within private 5G networks. The diversity and complexity of these threats highlight the need for multifaceted and adaptive security solutions.

5. **Proposed Solutions**: The studies reviewed suggest a variety of solutions, including enhanced authentication frameworks, the adoption of zero-trust architectures, and specialized countermeasures for specific threats. While some studies advocate for a comprehensive approach, such as the SDP framework, others focus on more targeted interventions, such as real-time detection algorithms for fake base stations. This diversity underscores the importance of an integrated, layered security strategy.

6. **Sector-Specific Security Concerns**: Several studies addressed the unique security requirements of specific sectors, such as smart healthcare, where confidentiality and real-time communication are critical. While other studies provide generalizable security frameworks, the need for tailored solutions specific to industry requirements is emphasized.

Overall, the findings underscore the complexity of securing private 5G networks. They emphasize the importance of tailored, adaptive, and collaborative approaches, combining advanced security technologies, regulatory reform, and industry-specific solutions to address the identified vulnerabilities and ensure the resilience of private 5G networks. Table 5 will present security best practices for private 5G networks, highlighting key strategies for mitigating security vulnerabilities and ensuring robust network protection.

Table 5

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 & Prevention Systems (IDPS)	Monitors network traffic for anomalies and mitigates potential threats.	Needs proper tuning to reduce false positives.	Crucial for identifying and blocking security breaches.
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.

Note. This data was collected from various literature. All authors have been cited accordingly.

6. Security Challenges in Private 5G Networks

Private 5G networks, while offering significant advantages in performance, reliability, and control, also introduce unique security challenges that must be addressed to ensure their safe and effective operation. These challenges arise from the natural characteristics of 5G technology, the specific requirements of private networks, and the evolving cyber threat landscape. As enterprises and industries increasingly adopt private 5G networks for critical communication needs, understanding and mitigating these security risks become paramount. One of the primary challenges is the expanded attack surface, as private 5G networks are typically deployed in industrial settings such as manufacturing plants, ports, and smart cities, involving a vast number of connected devices and IoT endpoints (Alanazi, 2023). Each device represents a potential entry point for cyber attackers, and the diversity of these endpoints, ranging from sensors and actuators to autonomous vehicles and smart infrastructure makes it difficult to enforce consistent security policies. Attackers can exploit vulnerabilities in weaker devices to gain unauthorized access, compromise sensitive data, or disrupt network operations(Adil et al., 2024). Another critical concern is network slicing security, a fundamental feature of 5G that allows multiple virtual networks to be created within a shared physical infrastructure. In private 5G deployments, different slices are tailored for specific applications such as industrial automation, IoT, and enhanced mobile broadband. However, ensuring the isolation of these slices, preventing cross-slice attacks, and enforcing slice-specific security policies present significant challenges (Tripathi et al., 2022). A security vulnerability in one slice could potentially be exploited to affect other slices, undermining the overall integrity of the network. Existing research highlights the risks associated with inter-slice resource allocation, lateral movement of threats, and improper enforcement of slice-specific security controls (Tripathi et al., 2022).

Edge computing security is another area of concern, as private 5G networks increasingly leverage edge computing to reduce latency and enhance performance. While edge computing enables faster data processing closer to the source, it also introduces new security vulnerabilities(Tripathi et al., 2022). Edge nodes, which are often distributed across different locations, may lack the robust security controls found in centralized data centres. These nodes are susceptible to both physical and cyber-attacks and ensuring the secure transmission of data between the edge and core network is crucial(Ji et al., 2024). Additionally, the decentralized nature of edge computing makes real-time monitoring and incident response more complex, requiring advanced threat detection mechanisms such as AI-driven anomaly detection (Kim et al., 2023). The integration of legacy systems with private 5G networks also presents security risks. Many organizations deploy private 5G alongside existing IT and operational technology (OT) infrastructure, which may not be designed to meet modern security standards. Legacy systems often contain outdated security protocols, unpatched vulnerabilities, and lack support for advanced encryption and authentication mechanisms (Tripathi et al., 2022). Attackers can exploit these weaknesses to gain unauthorized access, manipulate network traffic, or disrupt services. A comprehensive security strategy must include robust compatibility measures, network segmentation, and regular vulnerability assessments to mitigate risks associated with legacy infrastructure.

Insider threats pose additional security challenges, as authorized personnel, including employees, contractors, and third-party vendors, may intentionally or unintentionally compromise network security. Weak access controls, poor credential management, and insufficient monitoring mechanisms increase the risk of insider threats (Angin et al., 2022). Implementing multi-factor authentication (MFA), role-based access control (RBAC), and behavioural analytics can help detect and mitigate insider threats before they lead to security breaches. Regular security awareness training and stringent access policies are also crucial in minimizing the human factor in security risks. The evolving cyber threat landscape further complicates security in private 5G networks. Cyber adversaries continuously develop

sophisticated attack techniques, including advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and ransomware campaigns (Ahad et al., 2023). Private 5G networks, due to their high-speed, low-latency capabilities, become attractive targets for cybercriminals, state-sponsored attackers, and industrial spies. Security frameworks must incorporate proactive defence mechanisms such as real-time threat intelligence, automated security orchestration, and AI-driven anomaly detection to combat emerging threats. Additionally, continuous security updates, vulnerability patching, and incident response preparedness are essential to maintaining a strong security posture.

Finally, monitoring and incident response in private 5G networks remain challenging due to their distributed nature. Traditional security monitoring solutions may not be sufficient to handle the scale and complexity of private 5G environments, particularly in deployments involving edge computing and industrial IoT(Djuitcheu et al., 2023). Effective security monitoring requires a combination of real-time threat detection, automated response mechanisms, and forensic capabilities to analyse security incidents and prevent future attacks. The adoption of zero-trust architectures and security information and event management (SIEM) solutions can enhance visibility and response capabilities.

Therefore, securing private 5G networks requires an integrated approach that encompasses technical, operational, and human-centric security measures. Organizations must implement strong encryption, secure authentication protocols, network segmentation, and continuous monitoring to mitigate risks. As private 5G adoption continues to grow, staying ahead of evolving threats through stringent security strategies, advanced threat intelligence, and adherence to best practices will be critical to ensuring the resilience and integrity of these networks. Table 6 presents a high-level overview of security concerns in private 5G networks.

Table 6

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 & Response	The challenge of real-time threat detection, automated response, and forensic analysis in a highly distributed private 5G environment.
Authentication & Access Control	Enforcing robust identity verification for users, devices, and services to prevent unauthorized access
Regulatory & 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.

Note. The data in this table was collected through various literature. Authors have been cited through section 6.

6.1. Threats to Data & Services in Private 5G Network

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

Eavesdropping and Privacy Leaks:

Eavesdropping poses a substantial risk to the confidentiality, integrity, and availability of data within private 5G networks, making it a critical concern in safeguarding sensitive information(Hasan et al., 2021). By intercepting communications, attackers gain unauthorized access to sensitive data, including personal information, corporate secrets, and financial transactions(Ahad et al., 2023). This intrusion directly undermines confidentiality, as intercepted data can be exploited for malicious purposes such as identity theft, corporate espionage, or financial fraud. With private 5G networks increasingly being deployed across industries like healthcare, finance, and manufacturing, the risk of eavesdropping escalates significantly, given the high volume of sensitive data transmitted in real time. Attackers often leverage network vulnerabilities through techniques such as man-in-the-middle (MITM) attacks, packet sniffing, or exploiting insecure communication channels to intercept data in transit(Ahad et al., 2023). Unencrypted or poorly encrypted data becomes an easy target, leaving it vulnerable to exploitation. This not only compromises confidentiality but also poses potential risks to integrity, as attackers may tamper with intercepted data before relaying it to its destination.

For instance, altering financial transactions or modifying medical records could lead to devastating consequences for individuals and organizations alike. The impacts of eavesdropping extend beyond data interception. For individuals, the exposure of personally identifiable information (PII) can result in severe privacy breaches, leading to identity theft and financial losses(Alanazi, 2023). For organizations, the risks are equally dire, as corporate espionage could lead to the theft of confidential business strategies, intellectual property, or proprietary research. Such breaches compromise organizational integrity, eroding trust in the network's ability to safeguard sensitive data and resulting in financial losses and reputational damage. Furthermore, availability may also be indirectly affected by eavesdropping. Attackers who gain access to sensitive information might exploit it to disrupt services, whether by overloading network resources or initiating follow-up attacks, such as denial-of-service (DoS). The presence of malicious actors within the network can degrade performance, cause interruptions, or lead to prolonged downtime, undermining user trust and operational reliability. Privacy leaks exacerbate these risks by exposing data through vulnerabilities in the network's design, such as inadequate encryption, misconfigured access controls, or weak data handling procedures(Adil et al., 2024). These lapses can unintentionally expose sensitive information to unauthorized parties, compounding risks to confidentiality and integrity. In private 5G networks, where vast amounts of sensitive data are transmitted regularly, even minor lapses in privacy controls can lead to significant breaches, compromising both user privacy and organizational integrity(Hasan et al., 2021).

Why it is critical for data:

In a corporate environment, threats to the confidentiality, integrity, and availability (CIA) of data are particularly alarming in industries such as healthcare, finance, and manufacturing, where the secure transmission and storage of sensitive information are crucial (Suraci; et al., 2021). These sectors depend on robust data protection mechanisms to maintain operational continuity, safeguard customer privacy, and comply with stringent regulatory standards. Eavesdropping attacks in private 5G networks directly undermine data confidentiality, enabling malicious actors to intercept sensitive communications and exploit them for malicious purposes. In the healthcare industry, such attacks can have profound consequences, exposing patient health records and violating regulations like the Health Insurance Portability and Accountability Act (HIPAA). The breach of such highly sensitive data can lead to personal harm for patients and legal ramifications for healthcare providers (Ahad et al., 2023).

Similarly, in the financial sector, intercepted communications could reveal private banking transactions or credit card details, resulting in identity theft, fraudulent activities, and significant financial losses for both individuals and institutions. For manufacturing organizations, eavesdropping poses a threat to intellectual property, trade secrets, and proprietary designs.

Unauthorized access to this type of information could provide competitors with an unfair advantage, undermining the affected organization's market position and resulting in severe economic losses. Beyond financial implications, eavesdropping can cause irreparable reputational harm. Organizations found to be negligent in protecting sensitive data may lose consumer trust and face public scrutiny, eroding their standing in the market. Legal liabilities add another layer of concern, especially in jurisdictions governed by strict data protection laws such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States. Breaches of confidentiality can result in lawsuits, regulatory penalties, and hefty fines, further straining the affected organizations. The threat of eavesdropping extends beyond isolated incidents to systemic vulnerabilities within private 5G networks. These networks, designed to handle high volumes of real-time data, are particularly susceptible to exploitation if appropriate safeguards are not in place. Weak encryption, inadequate access controls, and insufficient monitoring mechanisms leave these networks exposed to prolonged and undetected attacks. Malicious actors leveraging advanced eavesdropping techniques, such as man-in-the-middle (MITM) attacks, can intercept and manipulate data in transit, undermining its integrity. For instance, altered financial transactions or tampered medical records can lead to faulty decision-making and catastrophic consequences for organizations and individuals. Furthermore, eavesdropping attacks have the potential to compromise the availability of data and services. By exploiting intercepted data, attackers could launch subsequent attacks, such as denial-of-service (DoS), to disrupt the network's functionality. This disruption can result in prolonged downtime, operational inefficiencies, and significant financial repercussions.

The insidious nature of eavesdropping lies in its ability to operate covertly, often going undetected for extended periods while attackers continuously intercept and exploit sensitive data (Suraci; et al., 2021). As private 5G networks increasingly facilitate critical operations, the risk of undetected eavesdropping attacks grows. Consequently, implementing robust security protocols, including strong encryption, stringent access controls, and proactive monitoring, is essential to mitigating the threats posed by eavesdropping. These measures are imperative to safeguarding the CIA of data within private 5G environments and maintaining trust in their secure operation.

Spoofing and Fake User Equipment (UE):

Spoofing attacks, particularly those involving fake user equipment (UE), pose a significant threat to the confidentiality, integrity, and availability of data within private 5G networks (Tripathi et al., 2022). These attacks exploit vulnerabilities in the identity verification process by impersonating legitimate devices, allowing attackers to gain unauthorized access to network resources, manipulate sensitive data, and remain undetected. The consequences of such attacks are far-reaching, as they extend beyond simple data manipulation to include breaches of confidential information and potential service disruptions, making spoofing particularly insidious. Confidentiality is compromised when attackers utilize fake UEs to access sensitive information transmitted across the network. By mimicking legitimate devices, attackers can intercept private communications or access confidential organizational data without detection. In corporate environments, for instance, this could lead to the exposure of trade secrets or sensitive customer information (Angin et al., 2022).

In healthcare settings, attackers could gain unauthorized access to patient health records or other personally identifiable information, violating privacy regulations and exposing organizations to legal penalties. Similarly, financial institutions are at risk of exposing private banking transactions or credit card details, leading to identity theft, fraud, and significant financial losses(Alanazi, 2023). The integrity of data is equally threatened by spoofing and fake UEs. Attackers can introduce falsified or altered data into the network, which disrupts the accuracy of critical information used in decision-making processes. For example, in industrial settings, manipulated data could result in improper machine configurations, production errors, or even hazardous conditions. In the financial sector, fake UEs could submit false transactions, compromising account balances, transaction histories, and financial reports, which can lead to operational and reputational damage. Beyond confidentiality and integrity, availability is also at risk. Fake UEs can contribute to service disruptions by overloading network resources, participating in denial-of-service (DoS) attacks, or interfering with legitimate communications. For example, a swarm of fake UEs could monopolize bandwidth, reducing the availability of network resources for legitimate users. This not only impacts the seamless operation of the network but also undermines user trust in the reliability of the system. These attacks can persist undetected for extended periods, creating vulnerabilities within the network and enabling attackers to execute further malicious actions (Wani et al., 2024).

As private 5G networks become increasingly interconnected, the consequences of spoofing and fake UE attacks can ripple across multiple sectors, from industrial automation to healthcare and finance. Addressing these risks requires a comprehensive approach that emphasizes advanced authentication mechanisms, real-time threat monitoring, and robust access control systems. Strengthening the verification process for user equipment and implementing monitoring measures are essential for mitigating the risks posed by spoofing and fake UEs. Furthermore, fostering collaboration between network operators, equipment manufacturers, and security experts is crucial for developing innovative solutions that address the evolving threat landscape of private 5G networks (Tripathi et al., 2022). This comprehensive approach will ensure the confidentiality, integrity, and availability of data, safeguarding the secure and reliable operation of private 5G ecosystems.

Why it is critical for data:
The integrity of data is paramount in environments where reliable information supports critical processes. Spoofing and fake user equipment (UE) attacks directly threaten data integrity by introducing false or manipulated data into private 5G networks (Tripathi et al., 2022). These attacks exploit weaknesses in authentication mechanisms, allowing attackers to impersonate legitimate devices and compromise the accuracy of data being transmitted (Cui et al., 2024). In environments like manufacturing, spoofing or fake UE devices can compromise sensor data used to control machinery, leading to inefficiencies, increased costs, and potential safety risks (Aijaz, 2020).

Similarly, in smart city infrastructures, where private 5G networks manage interconnected systems such as traffic signals or energy grids, spoofing attacks can cause widespread disruption. Fake UE devices could introduce misleading data into traffic systems, creating unsafe conditions and misdirecting vehicle flow. In energy systems, manipulated data could lead to power imbalances or outages, undermining public trust in these essential services (Eswaran & Honnavalli, 2023). The hidden danger of spoofing and fake UE lies in their ability to operate covertly, introducing false information into critical processes without detection. This not only jeopardizes data integrity but also erodes trust in decision-making processes that depend on accurate and timely information. To mitigate these risks and preserve the reliability of private 5G networks, implementing strong authentication mechanisms and validating the integrity of transmitted data are crucial steps (Ahmad et al., 2017).

Authentication Issues:
Authentication mechanisms are a cornerstone of securing private 5G networks(Ahad et al., 2023). However, weak or flawed implementations of these mechanisms can create critical vulnerabilities, allowing attackers to bypass security protocols and gain unauthorized access to sensitive systems. Exploiting authentication weaknesses enables attackers to infiltrate private 5G networks, granting them access to data repositories, communication channels, and storage systems without detection. This undermines both the confidentiality and integrity of the data these networks are designed to protect(Ahad et al., 2023). The risk posed by authentication issues is amplified by the distributed nature of private 5G networks, which often encompass thousands of interconnected devices and endpoints(Ahad et al., 2023). Each device represents a potential attack vector, and if attackers can compromise even a single endpoint, it can serve as an entry point for broader exploitation.

One particularly critical challenge is maintaining strong, reliable authentication across a diverse array of devices, ranging from IoT sensors to industrial equipment. Unlike traditional networks, private 5G networks often integrate devices with varying capabilities and security requirements. Devices with limited computational power or outdated firmware may not support robust authentication protocols, creating weak links within the network. Attackers can exploit these weak points to gain unauthorized access, exposing sensitive data and enabling malicious activities, such as eavesdropping or data tampering(Cui et al., 2024). Moreover, authentication flaws can have cascading effects on the overall security posture of the network. Once an attacker bypasses authentication, they may gain administrative privileges, allowing them to modify configurations, access critical systems, or disable security measures. This level of access not only threatens data confidentiality and integrity but can also impact data availability by enabling denial-of-service (DoS) attacks or other forms of disruption(Cui et al., 2024).

Why it is critical for data:
Authentication is a fundamental component in protecting sensitive data, acting as the first line of defence against unauthorized access(Djuitcheu et al., 2023). In the context of private 5G networks, weak or flawed authentication mechanisms create vulnerabilities that attackers can exploit to compromise the confidentiality, integrity, and availability of data. When authentication is bypassed or compromised, malicious actors gain unrestricted access to critical systems and sensitive data, undermining the security framework of the network. From a confidentiality standpoint, inadequate authentication allows attackers to intercept or steal sensitive information, such as proprietary business data or personally identifiable information (PII) (Ji et al., 2024).

This breach exposes organizations and individuals to risks like identity theft, corporate espionage, and privacy violations. Similarly, integrity is jeopardized when weak authentication permits unauthorized access to alter or manipulate data. For instance, attackers can introduce falsified information into operational systems, which could disrupt decision-making processes and lead to financial losses or safety risks. Finally, weak authentication also impacts availability, as attackers can exploit the lack of strong security controls to initiate denial-of-service (DoS) attacks or disable critical services, leading to operational downtime and reduced reliability of the network. Given the risks to the CIA of data, implementing strong authentication protocols, such as multi-factor authentication and real-time monitoring, is critical to ensuring secure access and minimizing the threat of unauthorized intrusion. Without robust authentication measures, private 5G networks remain vulnerable to sophisticated

attacks that can have far-reaching consequences for organizations and individuals alike(Djuitcheu et al., 2023).

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

Distributed Denial-of-Service (DDoS) Attacks:

Distributed Denial-of-Service (DDoS) attacks represent a critical threat to the availability of services in private 5G networks, targeting their ability to deliver uninterrupted connectivity and reliable service to users. These attacks function by overwhelming network resources, such as bandwidth, servers, or other critical infrastructure components, with excessive traffic. This deluge of malicious traffic renders services inaccessible to legitimate users, causing significant disruptions to communication, automation, and operational processes(Ahad et al., 2023). The potential impact of DDoS attacks on private 5G networks is amplified by the nature of the services these networks support. Industries such as healthcare, manufacturing, and smart city operations rely on private 5G for real-time communication, automation, and decision-making processes. For example, in healthcare, private 5G enables the functioning of real-time patient monitoring systems and remote surgeries.

A DDoS attack that disrupts these services could lead to critical delays in patient care or life-threatening interruptions in medical procedures.(Ahad et al., 2023) Similarly, in manufacturing, DDoS attacks can halt automated production lines, causing delays, financial losses, and potential damage to equipment due to improper shutdown procedures(Corici et al., 2021). In smart city infrastructures, which depend on private 5G for traffic management, energy distribution, and public safety systems, the consequences of a prolonged DDoS attack can be catastrophic(Adil et al., 2024). Beyond availability, DDoS attacks can indirectly impact data confidentiality and integrity. Attackers often use DDoS attacks as a diversionary tactic, drawing attention away from more targeted efforts to infiltrate systems and exfiltrate sensitive data. The distributed nature of private 5G networks further complicates the mitigation of DDoS attacks(Javed & Niazi, 2019). With a highly interconnected architecture and numerous endpoints, these networks present a broad attack surface(Javed & Niazi, 2019). If robust security measures such as traffic filtering, rate limiting, and anomaly detection are not implemented, the ability to detect and neutralize DDoS attacks become significantly impaired. Moreover, the scalability of private 5G networks allows attackers to exploit the high bandwidth and low latency characteristics to amplify their attacks (Ahad et al., 2023).

Why is it critical for services:

Service availability is a cornerstone of mission-critical applications supported by private 5G networks, including autonomous vehicles, healthcare systems, and industrial IoT (Internet of Things). In such environments, uninterrupted access to services is vital to maintaining operational efficiency, safety, and productivity. Distributed Denial-of-Service (DDoS) attacks pose a significant risk to service availability by overwhelming network resources with malicious traffic, rendering critical services inaccessible to legitimate users(Ahad et al., 2023). For instance, in industrial IoT environments, where private 5G networks facilitate automated manufacturing processes, a DDoS attack can halt production lines, delay delivery schedules, and incur substantial financial losses. The interconnected nature of these systems means that disruptions in one part of the network can quickly cascade, resulting in widespread operational failures(Rostamia et al., 2023). Similarly, in healthcare, private 5G networks support applications such as real-time patient monitoring and remote surgeries.

A successful DDoS attack targeting these systems could lead to critical delays in patient care or interruptions in medical procedures, potentially resulting in life-threatening consequences(Ahad et al., 2023). Autonomous vehicles also rely on private 5G networks for seamless communication between vehicles and infrastructure. A DDoS attack disrupting these networks could lead to loss of vehicle

coordination, increased risk of accidents, and delays in transportation systems, posing significant risks to public safety (Ramezanpour et al., 2023). Moreover, the automated and highly interconnected nature of private 5G networks magnifies the impact of service disruptions. Even minor interruptions caused by DDoS attacks can propagate throughout the network, amplifying their effect and causing widespread system failures. This interconnectedness makes private 5G networks particularly vulnerable to such attacks, highlighting the critical need for robust security measures to ensure service availability(Aijaz, 2020). To mitigate these risks, private 5G networks must implement advanced threat detection and response mechanisms, such as real-time traffic analysis, anomaly detection, and automated mitigation strategies. Strengthening network resilience against DDoS attacks is essential to preserving the availability of services and maintaining the reliability of mission-critical applications.

Jamming Attacks:
Jamming attacks present a significant threat to the availability of services within private 5G networks by intentionally generating excessive noise or interference to disrupt the network's communication channels. This interference prevents legitimate devices from transmitting or receiving data effectively, severely affecting environments that rely on uninterrupted, high-speed connectivity, such as industrial automation, healthcare monitoring systems, and smart city infrastructure (Ahad et al., 2023; Corici et al., 2021). For instance, in industrial automation systems, where real-time communication between machines is essential for maintaining production efficiency, a jamming attack could halt manufacturing lines, resulting in costly downtime and operational disruption (Gaber et al., 2021). Similarly, in healthcare, where private 5G networks support continuous patient monitoring and telemedicine, jamming could delay critical medical interventions, jeopardizing patient safety (Ahad et al., 2023).

The consequences are similarly dire for smart city infrastructure, where systems such as traffic management, public safety communications, and utility monitoring rely heavily on stable 5G connectivity. A successful jamming attack could disable these services, putting public safety at risk and causing widespread chaos (Kitchin & Dodge, 2019). The susceptibility of 5G networks to jamming is heightened by the high-frequency bands they utilize, including millimetre-wave spectrum, which are more prone to attenuation and interference (Ji et al., 2024). This characteristic makes jamming a particularly effective attack vector, as attackers can exploit these vulnerabilities to disrupt communication more easily. Additionally, the high density of devices within private 5G networks exacerbates the issue; a single jamming attack could create widespread service unavailability across interconnected systems, impacting a range of critical applications (Ahad et al., 2023; Wen et al., 2022).

Why is it critical for services:
Jamming attacks pose a serious threat to the stability and reliability of wireless communication systems, particularly in sectors where continuous connectivity is essential. Industries such as smart grids, autonomous systems, and emergency response networks rely on real-time data exchange to ensure operational efficiency and safety. When a jamming attack disrupts communication, it can cause widespread outages, delays in critical operations, or even catastrophic failures, particularly in systems that demand high availability and low latency (Aijaz, 2020). For example, in smart grids, jamming attacks could hinder real-time monitoring and management of electricity distribution, potentially causing power outages and threatening energy security. In autonomous systems, such as self-driving vehicles or drones, communication disruptions could result in accidents or collisions due to the inability to exchange vital navigation and sensor data (Gaber et al., 2021). The increased vulnerability of 5G networks to jamming, particularly in the high-frequency spectrum, underscores the need for effective anti-jamming measures, such as frequency hopping, directional antennas, and advanced

interference detection algorithms. These strategies are crucial to ensuring service availability and preventing cascading disruptions in critical systems (Ahad et al., 2023).

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

Man-in-the-Middle (MITM) attacks represent a significant threat to the confidentiality, integrity, and availability of services within private 5G networks. These attacks occur when malicious actors intercept, eavesdrop on, or alter communications between devices and network components without the knowledge of the legitimate parties involved (Djuitcheu et al., 2023). The impact of MITM attacks is particularly severe in systems where secure data transmission is vital for service functionality, such as in financial transactions, healthcare operations, and industrial automation systems (Ji et al., 2024). From a confidentiality standpoint, MITM attacks enable attackers to gain unauthorized access to sensitive information, including login credentials, operational data, or personally identifiable information (PII) (Suraci; et al., 2021). For example, in financial systems, the interception of encrypted transactions can expose account details, facilitating fraudulent activities (Ahad et al., 2023). Additionally, MITM attacks undermine the integrity of services. Attackers may modify control commands or alter operational data in transit, leading to significant operational disruptions. In industrial settings, manipulated commands can cause machinery malfunctions, introduce defects into products, or even halt production lines altogether (Djuitcheu et al., 2023). Similarly, in healthcare systems, altered patient monitoring data can mislead medical professionals, potentially resulting in inappropriate or delayed treatments (Ahad et al., 2023).

Furthermore, MITM attacks pose a serious threat to service availability. Manipulated data or disrupted communications can lead to service outages or failures. For instance, tampering with synchronization signals in autonomous vehicles could lead to collisions or system disruptions. In critical infrastructures like energy grids, MITM attacks could compromise grid stability by sending erroneous control signals, triggering cascading failures (Ficzere et al., 2021). MITM attacks are executed using methods like DNS spoofing, session hijacking, or rogue access points, which exploit weaknesses in network protocols and authentication mechanisms. These vulnerabilities underscore the need for strong countermeasures such as end-to-end encryption, mutual authentication protocols, and intrusion detection systems (Ji et al., 2024).

Why is it Critical for Services:

In private 5G networks, particularly those supporting critical infrastructure, ensuring the integrity of communication between devices and services is paramount to maintaining operational reliability (Wen et al., 2022). Man-in-the-Middle (MitM) attacks, which involve the interception and manipulation of data in transit, pose a severe threat to this integrity (Corici et al., 2021). By altering communications, attackers can introduce errors, disrupt system functionality, or even cause complete service failures. This undermines the trustworthiness of transmitted information, making it difficult for operators to rely on network data for decision-making (Ahmad et al., 2017). The consequences of MitM attacks are particularly alarming in environments requiring real-time, precise communication, such as industrial automation, energy grid management, and healthcare monitoring systems. For example, manipulated control signals in industrial automation could cause machinery to operate outside safe parameters, leading to production stoppages or severe safety hazards (Ahad et al., 2023). Similarly, in critical energy infrastructures, tampered commands could destabilize grid operations, triggering cascading failures across the network (Ficzere et al., 2021). Such disruptions not only compromise service integrity but also threaten the broader operational stability of private 5G networks. To mitigate these risks, robust security mechanisms such as end-to-end encryption, mutual authentication, and real-time traffic

monitoring must be implemented to safeguard against MitM threats (Ji et al., 2024). Without these countermeasures, private 5G networks remain vulnerable to service disruptions, unauthorized data manipulation, and loss of trust in their operational reliability.

Fake Base Station Attacks:
Fake base stations (fake BS) pose a significant threat to the confidentiality, integrity, and availability (CIA) of services in private 5G networks. These rogue systems impersonate legitimate base stations by broadcasting system information with a stronger signal, deceiving user equipment (UE) into connecting to them (Wani et al., 2024). Once a UE is connected, attackers can exploit the connection to intercept sensitive communications, compromise data integrity, and disrupt service availability. Confidentiality is particularly at risk, as fake BS attacks often involve IMSI-catching techniques, which force UE to disclose subscriber identities such as the International Mobile Subscriber Identity (IMSI) (Ahad et al., 2023). This enables attackers to track users, compromise privacy, and facilitate further malicious activities (Wani et al., 2024). Additionally, weaknesses in access point selection algorithms at the physical layer make private 5G networks vulnerable to location privacy breaches, exposing sensitive user location data (Ahmad et al., 2017). These risks are further compounded in shared 5G environments, where cloud-based storage systems distribute sensitive data across jurisdictions with differing privacy regulations, making confidentiality protection even more complex (Ahmad et al., 2017).

Fake BS attacks also compromise the integrity of private 5G networks. By intercepting and modifying communications between UE and legitimate network components, attackers can manipulate unicast or paging messages, injecting false information, or altering control commands. This type of manipulation can result in service mismanagement, operational failures, or even intentional sabotage, which is particularly concerning for mission-critical applications such as healthcare and industrial automation (Wani et al., 2024). Moreover, fake BS attacks threaten service availability by redirecting UE away from legitimate base stations, effectively preventing access to essential services. This is especially critical in environments where uninterrupted connectivity is vital, such as emergency response systems or industrial manufacturing, where disruptions can lead to delays, financial losses, or even endanger human lives (Wani et al., 2024).

The involvement of multiple stakeholders in private 5G networks, including Virtual Mobile Network Operators (VMNOs) and Communication Service Providers (CSPs), further complicates security management. Differing security and privacy priorities among these entities make it challenging to enforce uniform security measures and ensure seamless service availability (Ahmad et al., 2017). Additionally, the reliance on shared infrastructure and cloud storage removes physical data boundaries, introducing jurisdictional privacy challenges when data is stored in countries with varying regulatory frameworks (Ahmad et al., 2017). These vulnerabilities underscore the need for robust countermeasures, including advanced fake BS detection mechanisms, stronger access controls, and collaborative security frameworks to mitigate the risks posed by fake BS attacks.

Why is it critical for services:
Fake base station attacks pose a significant risk to services within private 5G networks, particularly in environments where uninterrupted communication between mobile devices and network infrastructure is essential. When a device connects to a fake base station, attackers can exploit the connection to disrupt service availability, degrade network performance, or execute further malicious activities, ultimately jeopardizing the reliability and functionality of private 5G network services (Ahad et al., 2023). These disruptions are especially concerning for mission-critical applications, where delays

or failures can lead to severe consequences, including operational downtime and safety hazards. In industrial automation, healthcare systems, and emergency response networks, any interruption in service can compromise real-time operations, endanger lives, or result in financial losses. To mitigate these risks, deploying effective detection mechanisms and implementing robust countermeasures is essential to prevent unauthorized access and maintain the reliability and security of private 5G network services.

6.2. Use Case

Securing private 5G networks requires addressing several complex security challenges, particularly in the implementation of network slicing. One critical concern is slicing isolation bypass, a vulnerability that allows attackers to move laterally between network slices, breaching security boundaries and accessing unauthorized data or services (Djuitcheu et al., 2023). Since network slicing is a foundational feature of 5G, enabling multiple virtualized networks to operate on shared infrastructure, a failure in isolation mechanisms can lead to severe security breaches, particularly in mission-critical private 5G deployments such as industrial automation, healthcare, and smart grids. Network slicing leverages Software-Defined Networking (SDN) and Network Function Virtualization (NFV) to dynamically allocate resources for different applications and services (Lackner et al., 2023). While this provides flexibility and efficiency, it also introduces security risks. Attackers can exploit misconfigurations or vulnerabilities in the slice management system to gain unauthorized access, manipulate control commands, or conduct Denial-of-Service (DoS) attacks targeting specific slices. If a private 5G network is compromised through slice isolation bypass, it could lead to data leakage, service disruption, or even unauthorized control over critical infrastructure components.

Another major challenge in securing private 5G networks lies in regulatory and operational constraints, which create security gaps that adversaries can exploit. Differences in national regulations and spectrum licensing models introduce inconsistencies in security implementations, increasing the attack surface across jurisdictions (Ahokangas et al., 2021). Furthermore, local 5G network operators, especially those outside traditional telecom providers, may lack the security expertise and commercial agreements needed to ensure robust protection against emerging threats. Additionally, lengthy, and complex authorization processes for radio equipment can delay security updates, making private 5G networks vulnerable to evolving attack techniques. Security and privacy concerns further complicate data-sharing protocols, which must comply with both sector-specific regulations and national security interests (Ahokangas et al., 2021). Without harmonized security frameworks, private 5G networks risk exposure to cross-border cyber threats, particularly in environments where sensitive industrial or governmental data is processed.

A specific use case that highlights the security vulnerabilities of network slicing is Vehicle for Hire (VFH) applications. In these scenarios, network slicing is used to provide ultra-reliable and low-latency communication to support fleet management, navigation, and customer interactions. However, attackers can exploit vulnerabilities in slice isolation and handover (HO) mechanisms to disrupt services or conduct location-based attacks. For instance, when drivers deviate from predetermined optimal routes, the handover process may be disrupted, making the network more susceptible to signal jamming, rogue base stations, or unauthorized interception of communications. This can lead to degraded service quality, increased call drops, or even the exposure of real-time location data, which could be exploited for targeted cyber or physical attacks (Mejia et al., 2024).

Moreover, the integration of multi-layered contextual factors, such as traffic patterns, institutional rules, and human behaviour, introduces qualitative uncertainties that further complicate security measures. Attackers could leverage these unpredictable elements to bypass traditional security

protocols. Additionally, simulation frameworks such as the Ingolstadt Traffic Scenario for SUMO (InTAS), which are used to align real-time traffic dynamics with slice resource allocation strategies, present potential security risks if not properly secured (Mejia et al., 2024). If adversaries gain access to these systems, they could manipulate traffic simulations, disrupt fleet coordination, or launch attacks that impact both physical and digital infrastructure.

To mitigate these security risks, private 5G networks must implement strong slice isolation mechanisms, advanced intrusion detection systems, and AI-driven traffic anomaly monitoring(Tripathi et al., 2022). Furthermore, regulatory bodies should work towards harmonized security policies to ensure consistent protections across different jurisdictions. Addressing these vulnerabilities is essential to maintaining the confidentiality, integrity, and availability of services within private 5G networks and securing mission-critical applications(Ji et al., 2024).

7.Mitigations

This section explores the mitigation strategies proposed in the literature to address the multitude of security vulnerabilities present in private 5G networks. With their increasing use in mission-critical applications across industries like healthcare, industrial automation, and smart grids, private 5G networks face significant threats that could undermine the confidentiality, integrity, and availability (CIA) of their services. Securing these networks requires a robust and evolving set of solutions. This section synthesizes the key mitigation approaches identified in the research, focusing on advanced encryption methods, sophisticated intrusion detection and prevention systems (IDS/IPS), and robust authentication protocols that collectively strengthen the security posture of private 5G networks. Emerging technologies, including quantum-resistant cryptography, machine learning-based anomaly detection, and multi-factor authentication, offer additional layers of protection. These strategies aim to mitigate a wide range of threats such as unauthorized access, data breaches, denial-of-service (DoS) attacks, and communication disruptions caused by jamming.

Each mitigation approach is evaluated within the context of private 5G networks, considering their capacity to address unique challenges like device heterogeneity, dynamic network slicing, and the integration of edge computing and virtualization technologies. For instance, while encryption provides foundational security for data in transit and at rest, its computational overhead may impact the performance of latency-sensitive applications, such as autonomous vehicles. Similarly, IDS/IPS systems must be fine-tuned to detect sophisticated attacks, such as zero-day exploits, while minimizing false positives that could disrupt operations. The section also highlights the challenges in implementing these mitigation strategies, particularly scalability, interoperability, and the evolving nature of cyber threats. Deploying advanced cryptographic solutions across diverse network components, including IoT devices with limited computational power, necessitates careful optimization. Additionally, the involvement of multiple stakeholders, such as Communication Service Providers (CSPs), Virtual Mobile Network Operators (VMNOs), and cloud infrastructure providers complicates security responsibility management and policy enforcement.

Through an in-depth review of the current literature, this section provides a comprehensive overview of the effectiveness of various mitigation strategies in the context of private 5G networks. It identifies not only the strengths of these strategies but also the limitations and challenges that need to be addressed. This analysis sets the stage for future research into adaptive, scalable, and cost-effective security solutions that can ensure the continued reliability and security of private 5G networks as new threats and technological advancements emerge. Ultimately, it emphasizes the importance of a multi-layered security framework that evolves to meet the needs of both current and future private 5G environments.

Jamming Attacks

Jamming attacks pose a significant threat to private 5G networks by disrupting communication and degrading service availability. To counter these threats, a multi-layered and adaptive defence strategy is essential. One of the most effective measures is spread spectrum techniques (SST), which scatter transmitted signals across a broad frequency range. This reduces an attacker's ability to focus interference on a specific channel, thereby preserving communication integrity (Corici et al., 2021). Complementing SST, frequency hopping techniques dynamically change communication channels, making it significantly more difficult for attackers to locate and target specific frequencies (Angin et al., 2022). Another critical mitigation measure is random key distribution, which frequently alters encryption keys to prevent attackers from predicting and disrupting communication. This dynamic approach

enhances the security of communication channels, particularly against targeted interference attacks (Corici et al., 2021). Control channel protection is equally crucial, as attackers often target these channels with high-powered signals. By employing encryption and advanced frequency modulation mechanisms, private 5G networks can fortify these channels against disruption, ensuring continued operation (Angin et al., 2022).

Beyond practical defences, self-recovery mechanisms play a pivotal role in restoring private 5G networks following an attack. These mechanisms help minimize service disruptions and mitigate the impact of data loss, ensuring the availability of critical services (Wani et al., 2024). The heterogeneity of IoT devices within private 5G networks further necessitates tailored solutions. A flexible approach that accounts for the varying susceptibilities of different devices ensures comprehensive protection across the network (Alanazi, 2023). At the application level, incorporating redundancy mechanisms can safeguard critical services against disruptions caused by jamming. By ensuring backup communication paths, redundancy enhances network resilience, allowing continued operation even during an attack (Pirayesh & Zeng, 2022). At the network layer, power control mechanisms dynamically adjust transmission power to minimize interference and maintain stable connectivity. A key component of jamming attack mitigation is the deployment of Intrusion Detection and Prevention Systems (IDPS). These systems continuously monitor network traffic in real time, identifying irregularities indicative of jamming attempts. By analysing traffic patterns, IDPS can automatically trigger countermeasures, such as switching communication channels or deploying signal-jamming countermeasures to mitigate interference. This approach helps maintain the integrity and availability of communication channels (Corici et al., 2021; Pirayesh & Zeng, 2022).

Additionally, maintaining regular software and hardware updates is critical in defending against evolving jamming tactics. Attackers often exploit known vulnerabilities in outdated systems; therefore, timely patching and updates strengthen network security and resilience against emerging threats (Ji et al., 2024; Pirayesh & Zeng, 2022). By integrating these defensive strategies, spread spectrum techniques, frequency hopping, random key distribution, control channel protection, redundancy mechanisms, IDPS deployment, power control, and continuous system updates, private 5G networks can establish a robust, multi-layered defence. This comprehensive approach safeguards network integrity and availability, ensuring resilience against jamming attacks while maintaining uninterrupted communication services for mission-critical applications.

Man-in-the-Middle (MITM) Attacks

Mitigating Man-in-the-Middle (MITM) attacks in private 5G networks requires a comprehensive, multi-layered security approach. One of the fundamental defences is network isolation, which restricts unauthorized access and reduces the risk of information leakage. By implementing network segmentation and enforcing strict isolation policies, organizations can prevent attackers from intercepting or altering communication channels, especially within private or campus networks (Badhwar, 2021; Djuitcheu et al., 2023). A multi-layered defence strategy strengthens security by integrating network-level protections such as intrusion detection systems (IDS) and end-to-end encryption with application-specific safeguards and user awareness training. Regular updates and patching of system components, software, and firmware are essential to addressing known vulnerabilities before they can be exploited (Alanazi, 2023). Strong authentication mechanisms, particularly multi-factor authentication (MFA), play a pivotal role in preventing unauthorized access. MFA ensures that only legitimate

users can enter the network, reducing the risk of stolen credentials being leveraged for MITM attacks (Alanazi, 2023). Similarly, end-to-end encryption protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPSec), safeguard the confidentiality and integrity of data during transmission, making it significantly harder for attackers to intercept or manipulate communications.

To further strengthen defences, advanced Intrusion Detection and Prevention Systems (IDPS) actively monitor network traffic, detect anomalies, and automatically respond to unauthorized interception attempts in real time (Corici et al., 2021). In addition to technical controls, organizations should establish a comprehensive incident response plan that ensures swift detection and mitigation of MITM attacks. Clearly defined response procedures help restore network integrity and minimize disruption to critical communications. User education and awareness training serve as additional safeguards against social engineering tactics, such as phishing, which are frequently used to initiate MITM attacks (Alanazi, 2023). Employees and users should be trained to recognize suspicious activity and potential attack vectors.

Blockchain technology provides an additional layer of security by enabling decentralized verification of public keys, thereby reducing the risk of key compromise or data hijacking (Lin et al., 2023). Its immutable nature further ensures the integrity of communications, making blockchain a valuable tool in defending against MITM attacks (Alanazi, 2023). Mutual authentication between network entities like user devices and base stations which further strengthens security by preventing unauthorized actors from impersonating legitimate devices (Corici et al., 2021). Additionally, continuous monitoring mechanisms, supported by machine learning-based anomaly detection, enhance real-time threat detection and enable defences against suspicious network activities. Finally, fostering collaboration among researchers, industry stakeholders, and cybersecurity professionals facilitates threat intelligence sharing and the development of advanced security measures to counter emerging MITM techniques (Ji et al., 2024). By integrating these defences network isolation, encryption, authentication, IDPS, blockchain security, anomaly detection, and practical threat intelligence sharing private 5G networks can establish a robust, adaptive security framework. This ensures the security, integrity, and availability of critical communications, effectively mitigating MITM attacks in evolving 5G environments.

Denial of Service (DoS) Attacks

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks present a critical security challenge for private 5G networks, particularly due to the large number of interconnected devices they support (Corici et al., 2021). These attacks aim to exhaust network resources, making them unavailable to legitimate users and causing severe service disruptions. In a DoS attack, a lone source floods a server with TCP, UDP, or ICMP packets, overwhelming its processing capacity. In contrast, a DDoS attack involves multiple compromised devices coordinating to target the network simultaneously. Private 5G networks, which power mission-critical applications such as industrial automation, smart healthcare, and autonomous systems, are particularly vulnerable to such large-scale disruptions (Wen et al., 2022). Attackers can exploit network slicing, control plane operations, and radio access components to severely degrade service availability (Ahad et al., 2023).

Mitigating DDoS attacks in private 5G networks requires a multi-layered approach that integrates detection, prevention, and resilience strategies. Intrusion Detection and Prevention

Systems (IDPS) play a crucial role in monitoring network traffic in real time, identifying anomalies such as sudden surges in requests or malicious packet floods. By blocking suspicious traffic before it overwhelms network resources, IDPS ensures that legitimate users maintain access to services (Corici et al., 2021). Advanced DDoS mitigation techniques, such as rate limiting, traffic filtering, and DNS server protection, further enhance network security. These methods restrict the number of requests per second, filter out suspicious traffic patterns, and protect core network services from being overwhelmed (Corici et al., 2021).

To improve resilience, private 5G networks can deploy anti-DDoS hardware, increase bandwidth, establish redundant infrastructure, and implement network monitoring. Anti-DDoS hardware appliances absorb malicious traffic before it affects mission-critical services, while redundant network paths ensure uninterrupted communication even during an ongoing attack (Corici et al., 2021). Additionally, securing network slicing and edge computing resources is essential, as private 5G deployments often rely on these components to allocate dedicated bandwidth for high-priority applications such as telemedicine and industrial automation. DDoS attacks targeting radio access networks (RAN) and slicing mechanisms can cripple essential services. Implementing adaptive traffic management, edge-based anomaly detection, and cloud security controls helps maintain service availability under attack conditions (Ahad et al., 2023). By combining real-time detection, filtering, and infrastructure resilience, private 5G networks can effectively mitigate DoS and DDoS attacks, ensuring the continuous availability of critical services even under hostile conditions.

Spoofing Attacks

Mitigation strategies to address spoofing attacks focus on enhancing the integrity and authentication mechanisms of private 5G networks. Techniques such as mutual authentication, where both the user and the network verify each other's identity, are essential to prevent unauthorized access. Cryptographic methods, including public key infrastructure (PKI) and digital certificates, play a critical role in ensuring the authenticity of communication parties. Additionally, leveraging physical layer security measures, such as channel state information (CSI)-based authentication, provides an added layer of protection by utilizing unique characteristics of the wireless channel. These measures ensure that only legitimate devices can communicate within the network, reducing the risk of identity spoofing and session hijacking(Alanazi, 2023).

Research has also highlighted the importance of incorporating machine learning-based anomaly detection systems to identify and respond to spoofing attempts in real time (Alanazi, 2023). These systems analyse network traffic patterns and signal characteristics to detect deviations indicative of malicious activity, allowing for threat mitigation. Furthermore, regular updates to software and firmware are crucial to patch vulnerabilities that could be exploited in spoofing attacks. Attackers often exploit outdated security protocols, making continuous updates an essential component of network defence. The findings from this review emphasize the pervasive threat of spoofing in private 5G networks and the necessity of implementing a combination of technological and procedural safeguards to mitigate its impact. The complexity and adaptability of spoofing attacks demand ongoing research and collaboration among stakeholders to develop comprehensive and effective defence mechanisms. Ensuring network security in private 5G environments requires a multi-layered approach that evolves alongside emerging threats and attack techniques.

Fake User Equipment Threats

Mitigating threats posed by fake user equipment (UE) is critical to maintaining the integrity and security of private 5G networks. One foundational strategy involves implementing robust authentication mechanisms, such as 5G Authentication and Key Management (AKA), to ensure that only legitimate UEs can access the network. By authenticating devices and establishing secure communication channels, private 5G networks can effectively minimize risks posed by impostor devices attempting to infiltrate the system (Mazroa & Arozullah, 2015). Furthermore, advanced security measures deployed at the network edge, including base stations, enable quicker detection and response to threats, thereby preventing unauthorized devices from gaining access (Wen et al., 2022). Another essential aspect of mitigation is securing the UE supply chain (Tripathi et al., 2022). Verifying the authenticity and integrity of devices before their deployment within a private 5G network is crucial, as a compromised supply chain can introduce malicious devices that undermine network security from the outset.

In addition to hardware validation, ensuring the isolation of private 5G networks from external environments plays a significant role in reducing exposure to fake UE threats. Isolated networks limit the attack surface, making it more difficult for adversaries to exploit vulnerabilities or infiltrate the system (Tripathi et al., 2022). Human behaviour also presents a significant challenge in addressing fake UE threats. Attackers frequently exploit users through phishing schemes or social engineering tactics, leading to unauthorized access or the deliberate installation of malicious software on legitimate devices. To counter this, implementing user awareness programs and training initiatives is essential. Educating users on identifying and avoiding potential threats significantly reduces the likelihood of successful exploits, particularly in private 5G environments where user actions play a critical role in network security (Djuitcheu et al., 2023). By integrating authentication mechanisms, supply chain security, network isolation, and user education, private 5G networks can establish a comprehensive defence against fake UE threats.

Fake Base Stations (FBS)

Mitigating fake base stations (FBS) requires a combination of proactive and reactive measures to prevent unauthorized access and communication disruptions within private 5G networks (Ahad et al., 2023). One of the primary preventative approaches involves digital signature-based authentication of system information messages by legitimate base stations (Purification et al., 2024). By digitally signing these messages, legitimate base stations ensure that only verified communications are accepted by user equipment (UE), preventing connections to unauthorized or malicious base stations. However, implementing such measures requires systematic changes in network protocols, including modifications in the UE, base stations, and core network infrastructure, making it a complex undertaking. Cryptographic approaches, such as the use of public key infrastructure (PKI), are also under consideration by the 3GPP (Purification et al., 2024). This strategy involves establishing and verifying the public key of base stations to enable secure authentication of communication exchanges. While 3GPP is still conceptualizing these requirements, PKI represents a robust mitigation framework that could significantly strengthen defences against FBS attacks (Alanazi, 2023). Despite its potential, cryptographic solutions require widespread standardization and systematic implementation, which may delay their deployment in real-world scenarios.

Reactive strategies focus on detecting and identifying fake base stations after they become operational. One effective detection method leverages UE behaviour when connected to an

FBS. By analysing Radio Resource Control (RRC) communications specifically the time and number of registration request packets researchers have demonstrated the ability to identify malicious base stations (Wani et al., 2024). This approach does not require modifications to the core network or legitimate base stations, making it more practical and deployable than cryptographic methods. Another critical mitigation strategy is the implementation of enhanced network monitoring and logging mechanisms (Corici et al., 2021). These systems can identify patterns indicative of unauthorized base station activity, such as unusual signal strength variations or irregular registration requests. Coupled with real-time alerts, these systems enable operators to take immediate action, such as isolating and shutting down the malicious base station (Alanazi, 2023). Additionally, enhancing UE-side security through multi-factor authentication or user-specific cryptographic keys can further protect against FBS. These methods reduce the likelihood of a UE establishing a connection to a rogue station and improve overall network resilience.

Implementing these measures across private 5G networks is particularly critical, as these networks often operate in highly sensitive environments such as industrial, healthcare, or government applications, where the risks of communication compromise are significantly higher (Chakraborty et al., 2023). A comprehensive defence strategy that integrates authentication measures, cryptographic solutions, real-time detection, and enhanced UE security will strengthen private 5G networks against FBS threats and ensure the integrity of communications.

Authentication Issues

Securing authentication processes in private 5G networks is critical for preventing unauthorized access and safeguarding sensitive information. Addressing authentication vulnerabilities requires a multi-faceted approach tailored to the unique characteristics of private 5G environments, particularly in industries such as smart healthcare and enterprise applications, where data security is paramount. To enhance security, private 5G networks can leverage advanced authentication protocols. Standalone non-public networks (SNPNs), for instance, employ a combination of Authentication and Key Agreement (AKA) and Extensible Authentication Protocol (EAP) mechanisms to strengthen user and device verification (Ahad et al., 2023). This layered approach ensures robust mutual authentication and secure key exchanges. Incorporating EAP-based authentication mechanisms into enterprise-owned user equipment (UE) further mitigates vulnerabilities and reduces the likelihood of attacks targeting devices (Ahad et al., 2023).

Remote user authentication is another critical consideration. Virtual Private Network Secure Service Client (VPN SSC) solutions enable secure connections for remote users in private 5G networks. Implementing multi-factor authentication (MFA) in tandem with VPNs enhances protection against unauthorized access, ensuring secure communication channels even in highly sensitive environments like smart healthcare (Tripathi et al., 2022). Dynamic authentication and authorization policies further bolster security by allowing real-time adaptability. These policies, supported by tools such as Access Graph User Plane Function (AGUPF) and Access Graph Policy Analyzer (AGPA), facilitate task-specific authentication and threat-specific adjustments. This dynamic approach enables private 5G networks to remain resilient against emerging threats and unauthorized access attempts (Ahad et al., 2023).

Additionally, secure key management plays a vital role in maintaining the integrity of private 5G network communications. The secure generation and exchange of cryptographic keys

between master base nodes (MeNB) and secondary base nodes (SgNB) ensure the authenticity and confidentiality of radio resource control (RRC) messages and user plane (UP) data, which prevents unauthorized interception and data tampering (Ahad et al., 2023). Finally, logging and monitoring access attempts provide an essential safeguard against authentication breaches. By analysing patterns of unauthorized access, organizations can identify potential vulnerabilities and respond proactively. For private 5G networks, implementing these controls is essential to maintaining the high-security standards expected in such environments (Ordóñez et al., 2019).

Unauthorised Access

Mitigating unauthorized access is a critical aspect of securing modern networks, requiring a combination of robust technical controls and procedural safeguards. One foundational strategy involves enforcing strong access control mechanisms to ensure that only authenticated and authorized users can access network resources. Implementing multi-factor authentication (MFA), role-based access control (RBAC), and least privilege principles significantly reduces the risk of unauthorized entry and data exposure(Alanazi, 2023). Network segmentation is another essential measure to limit unauthorized access and minimize the potential impact of security breaches. By dividing the network into isolated segments based on security levels and operational requirements, organizations can contain threats and prevent lateral movement by attackers. This approach is particularly effective in mitigating risks associated with threats like Man-in-the-Middle (MITM) attacks and Denial-of-Service (DoS) attacks, ensuring that critical systems remain protected even if one segment is compromised (Djuitcheu et al., 2023).

Physical security also plays a vital role in preventing unauthorized access to network infrastructure. Data centres, server rooms, and critical network equipment must be protected using access controls, surveillance systems, and intrusion detection mechanisms. Unauthorized physical access can lead to tampering, hardware-based attacks, or the introduction of malicious devices into the network. Beyond technical measures, human factors remain a significant risk in unauthorized access incidents. Attackers often exploit human vulnerabilities through phishing, social engineering, or insider threats. To address this, organizations should implement comprehensive security awareness programs and training initiatives, ensuring employees understand and follow security best practices(Djuitcheu et al., 2023). Additionally, continuous monitoring and regular security audits help identify and remediate vulnerabilities before they can be exploited, strengthening the overall security posture of the network. Effectively mitigating unauthorized access requires an integrated approach that combines technical, physical, and procedural security measures. By implementing these strategies, organizations can enhance their resilience against evolving threats and ensure that network resources remain secure and accessible only to legitimate users (Djuitcheu et al., 2023).

Eavesdropping and Privacy leaks

Eavesdropping attacks pose a significant threat to the confidentiality and integrity of data, particularly due to their passive nature, which makes detection challenging (Mohan et al., 2022). Since these attacks do not disrupt normal communication processes, robust countermeasures must be implemented at multiple levels of the communication infrastructure to mitigate the associated risks (Mohan et al., 2022). A primary defence against eavesdropping is the implementation of strong encryption protocols to secure transmitted data (Corici et al., 2021). Encryption ensures that even if an attacker intercepts

communications, the data remains unreadable without the appropriate decryption keys. Advanced encryption standards, such as the Advanced Encryption Standard (AES), provide highly effective protection for sensitive information and should be consistently applied across networks. Additionally, end-to-end encryption (E2EE) ensures that data remains secure throughout its entire transmission path, even when passing through potentially vulnerable channels.

Beyond encryption, network access control and segmentation further strengthen defences against eavesdropping. By limiting network access to authorized users and isolating critical systems into distinct security zones, organizations can minimize the attack surface available to adversaries. This approach restricts an attacker's ability to gain proximity to sensitive communication channels and enhances overall network security (Corici et al., 2021).
Continuous network monitoring is essential for detecting anomalies that may indicate potential eavesdropping activities. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) help identify unusual traffic patterns, while log analysis and real-time monitoring tools can reveal unauthorized attempts to access data (Tripathi et al., 2022). These measures enable organizations to detect and respond to threats before they result in significant data breaches.

Physical security also plays a crucial role in preventing eavesdropping attacks. Network infrastructure components such as cables, routers, and switches are common targets for physical tampering. Implementing strict access controls, securing critical hardware locations, and deploying surveillance systems can deter attackers from intercepting network traffic (Djuitcheu et al., 2023). Finally, secure authentication mechanisms add an additional layer of protection by verifying the identity of users and devices accessing the network. Techniques such as multi-factor authentication (MFA) and digital certificates ensure that only legitimate entities participate in communication, significantly reducing the risk of unauthorized interception (Ramezanpour et al., 2023). By combining encryption, network segmentation, continuous monitoring, physical security, and strong authentication measures, organizations can build a resilient defence against eavesdropping attacks, safeguarding the confidentiality and integrity of their communications.

8.Discussion and Future Directions

This SLR was conducted to investigate and analyse the security vulnerabilities inherent in private 5G networks. By employing a structured review process, this study synthesizes insights from a wide range of academic and industry research, providing a comprehensive exploration of the security threats, challenges, and risks associated with private 5G networks. The objective of this SLR is twofold: first, to identify and categorize the most critical and prevalent security concerns that threaten the integrity, confidentiality, and availability of private 5G networks; and second, to evaluate the practical implications of these vulnerabilities for key stakeholders, including network administrators, service providers, regulatory authorities, and end-users. These insights aim to bridge the gap between academic research and real-world applications, offering actionable recommendations for strengthening the security posture of private 5G environments. The findings of this review reveal a diverse array of security challenges. These include, but are not limited to, authentication and access control issues, risks associated with network slicing, vulnerabilities to Distributed Denial of Service (DDoS) attacks, and the emergence of sophisticated threats such as rogue base station deployments and signal overshadowing. Additionally, the review highlights the risks posed by insufficient encryption protocols, insider threats, and weaknesses in orchestration and network virtualization processes. These vulnerabilities underscore the urgent need for robust and adaptable security frameworks tailored to the unique architecture and operational requirements of private 5G networks.

The practical implications of these findings extend across multiple dimensions. For network administrators, identifying common attack vectors provides a roadmap for prioritizing security investments and implementing strong defence mechanisms. Service providers can leverage these insights to enhance the design and deployment of private 5G solutions, ensuring compliance with industry standards and regulatory requirements. Meanwhile, policymakers and regulatory bodies can utilize the findings to establish guidelines and frameworks that promote secure 5G network ecosystems while addressing critical gaps in spectrum allocation, authorization processes, and standardization efforts. Despite the breadth of research analysed, this review also uncovers significant gaps in the current body of knowledge. For example, there is limited empirical evidence on the long-term effectiveness of proposed mitigation strategies, particularly in dynamic threat landscapes. While several studies propose innovative solutions, such as Software-Defined Perimeter (SDP) architectures and moving target defence mechanisms, there is a lack of real-world validation of these approaches in private 5G environments. Moreover, specific application domains, such as smart healthcare and industrial IoT, require further exploration to address their unique security challenges comprehensively.

This SLR emphasizes the critical importance of continued research to address these gaps and advance the security of private 5G networks. By fostering collaboration between academia, industry, and regulatory entities, it is possible to develop resilient solutions that not only mitigate current vulnerabilities but also anticipate and defend against emerging threats. Through this comprehensive analysis, this thesis aims to contribute meaningfully to the ongoing discourse on private 5G network security, paving the way for more secure and robust network deployments in the future.

Overview of Findings: The systematic review identified a broad spectrum of critical security vulnerabilities that pose substantial risks to the integrity, confidentiality, and reliability of private 5G networks. These vulnerabilities, frequently discussed in the literature, underscore the complexity of safeguarding these advanced communication systems against evolving threats. Among the most prominent vulnerabilities is the risk of distributed denial-of-service (DDoS) attacks, which overwhelm network resources, rendering services inaccessible to legitimate users. These attacks are particularly concerning in private 5G networks due to their potential to disrupt mission-critical applications. Similarly, spoofing attacks were identified as a significant threat, where malicious actors impersonate

legitimate devices or users to gain unauthorized access, thereby compromising network integrity and security.

Unauthorized access emerged as another critical concern, with numerous studies emphasizing the vulnerabilities arising from weak authentication protocols and insufficient access control mechanisms. These issues are compounded in private 5G networks, where the high density of connected devices amplifies the risk of exploitation. Jamming attacks, which disrupt communication by flooding the network with interference, and man-in-the-middle (MITM) attacks, where attackers intercept and potentially alter communications between legitimate parties, further highlight the dynamic nature of threats facing these networks. Eavesdropping was frequently highlighted as a particularly insidious vulnerability, allowing attackers to intercept sensitive communications, extract confidential information, and compromise user privacy. Privacy leaks were another significant concern, with various studies pointing to the risks of unauthorized disclosure of personal or sensitive data. Such leaks are especially critical in applications such as smart healthcare and industrial IoT, where the consequences of compromised privacy could be severe.

The review also identified risks associated with tampering, where attackers manipulate data or devices to disrupt network functionality or introduce malicious activities. Fake base station attacks, a growing threat, were frequently cited in the literature. These attacks involve the deployment of rogue base stations by malicious actors to intercept user communications, harvest sensitive data, or facilitate further attacks on the network. The consistency with which these vulnerabilities were reported across multiple studies underscores their prevalence and the pressing need for robust, multi-layered security measures tailored to the unique architecture and use cases of private 5G networks. Addressing these vulnerabilities will require an approach that incorporates advanced authentication mechanisms, enhanced encryption protocols, and continuous monitoring to detect and mitigate potential threats in real time.

This analysis highlights the critical importance of developing comprehensive and adaptive security strategies to protect private 5G networks. Such strategies must address both the known vulnerabilities identified in this review and emerging threats that may arise as these networks continue to evolve. The findings presented here contribute to a growing body of knowledge aimed at improving the security and resilience of private 5G systems, ensuring their reliability in supporting critical applications and services.

8.3. Implications and Future Research Directions

8.3.1 Implications for Practice

The findings of this review carry significant implications for ensuring the security of private 5G networks, particularly considering the unique vulnerabilities and challenges fundamental to their deployment. Stakeholders must prioritize the design and implementation of comprehensive security protocols to address both established and emerging threats within the private 5G ecosystem. This requires adopting a multi-layered security approach, integrating advanced encryption methods, conducting regular security audits, enforcing robust access control mechanisms, and employing threat detection strategies.

I. Advanced Encryption Techniques: Encryption plays a critical role in safeguarding sensitive data transmitted across private 5G networks. Techniques such as end-to-end encryption and the use of cryptographic key pair mechanisms should be employed to protect user identities and network communications from interception or unauthorized access. For instance, encrypting the International Mobile Subscriber Identity (IMSI) or user equipment (UE) ID ensures that

such information cannot be exploited even if intercepted by attackers. Integration with established cryptographic libraries, like OpenSSL, enhances the security posture by facilitating the implementation of secure encryption, decryption, and key management practices (Alanazi, 2023).

II. Regular Security Audits and Continuous Monitoring: Conducting regular security audits is essential to identify and address vulnerabilities before they can be exploited. These audits should encompass both the physical and digital aspects of private 5G networks, including user equipment, base stations, and core network components. Continuous monitoring tools should be deployed to detect anomalies in real-time, enabling rapid responses to potential security breaches (Djuitcheu et al., 2023).

III. Robust Access Control Mechanisms: Implementing strict access control measures is another critical element of securing private 5G networks. This includes multi-factor authentication for user devices, role-based access control for network administrators, and segmentation of network slices to minimize the impact of potential breaches. User equipment should also be secured to prevent unauthorized access or manipulation by malicious actors (Hasan et al., 2021).

IV. Collaboration Across Stakeholders: The security of private 5G networks cannot be achieved in isolation. Collaboration between equipment manufacturers, service providers, and regulatory bodies is imperative to establish and maintain robust security frameworks. Equipment manufacturers should ensure that hardware and software components are designed with security as a foundational principle. Service providers must enforce security policies consistently, while regulatory bodies should set clear guidelines and standards to govern the deployment and operation of private 5G networks (Alanazi, 2023).

V. User Education and Awareness: A critical but often overlooked aspect of securing private 5G networks is user education. Human error remains a significant factor in security breaches. Therefore, training programs aimed at increasing awareness about potential threats and safe practices should be a mandatory part of any private 5G deployment strategy. Users should be informed about the risks of identity spoofing, manipulated user behaviour, and other vulnerabilities to reduce the likelihood of successful attacks (Djuitcheu et al., 2023).

In summary, the secure operation of private 5G networks demands a comprehensive and collaborative approach that addresses technical, organizational, and human factors. By integrating these practices, organizations can strengthen the resilience of private 5G networks against the rapidly evolving threat landscape and ensure their safe and reliable operation.

8.3.2 Future Research Directions

Despite the extensive research conducted on 5G networks, significant gaps persist in the literature, particularly regarding the security challenges specific to private 5G networks. While much of the current focus centres on public 5G networks, the unique characteristics, and requirements of private 5G deployments, such as those tailored for industrial automation, healthcare, or campus environments, remain underexplored. This lack of targeted research leaves critical questions unanswered about the vulnerabilities and attack vectors unique to private 5G networks. These environments often involve specialized implementations that differ fundamentally from public networks, introducing distinct security challenges that require tailored approaches.

One notable gap lies in the limited examination of specific vulnerabilities in private 5G environments. General 5G security concerns, such as Distributed Denial-of-Service (DDoS) attacks, eavesdropping, and authentication weaknesses, are well-documented in the literature. However, the distinct operational contexts of private 5G networks create additional risks. For instance, industrial deployments may face targeted attacks on network slicing or jamming threats aimed at disrupting mission-critical operations. Similarly, private campus networks may be more susceptible to internal threats or misconfigurations due to the controlled nature of access. Future research must prioritize in-depth case studies that evaluate how existing security protocols that have robust encryption, intrusion detection and prevention systems (IDPS), and multi-factor authentication perform in these environments. Understanding their limitations will help identify areas requiring enhancements or novel approaches.

Another critical gap is the absence of standardized security protocols tailored to private 5G networks. Unlike public networks, private deployments often operate under varying regulatory requirements and industry-specific constraints, such as stricter data privacy needs or integration challenges with legacy systems. Developing bespoke security frameworks that address these unique conditions is essential. For example, protocols that incorporate dynamic access controls, enhanced monitoring at the edge, and secure integration with IoT devices could significantly improve the resilience of private networks. Research should also investigate how security measures can be aligned with operational objectives to minimize disruption while ensuring comprehensive protection.

The role of emerging technologies, such as artificial intelligence (AI) and machine learning (ML), presents another critical research area. While these technologies hold the potential to enhance network security through real-time threat detection and adaptive responses, they also introduce new risks, such as vulnerabilities in AI algorithms or the potential for adversarial attacks. The dual nature of AI and ML in security contexts demands a nuanced understanding of how these technologies can be leveraged effectively while mitigating their risks. For example, future studies could explore AI-driven anomaly detection tailored to private 5G environments or investigate methods to secure ML models against tampering. In addition to the above, the following research gaps present opportunities for future exploration:

- **Insufficient Use of Threat Modelling**: There is a limited application of advanced threat modelling techniques, such as attack graphs, specifically for private 5G networks. One study analysed as part of this review demonstrated the utility of attack graphs for modelling enterprise network vulnerabilities and suggested their use for mitigating risks in standalone non-public networks (SNPNs). Expanding such methodologies to private 5G networks could significantly enhance threat assessment and mitigation efforts.
- **Moving Target Defence (MTD)**: Another gap identified is the lack of implementation of dynamic security mechanisms, such as MTD, which involve continually changing network

configurations to increase complexity for attackers. Future research could explore the feasibility and effectiveness of MTD for private 5G networks.

- **Automation of Security Models**: The automation of tools such as attack graph generation for private 5G networks is unexplored. Automating these models could streamline the identification of vulnerabilities and enhance real-time response capabilities.
- **Comparative Security Insights**: Limited research compares private 5G networks' security vulnerabilities with those of legacy networks, Wi-Fi, public 5G, and SNPNs. Studies that delve deeper into these comparisons could inform best practices and guide tailored security recommendations.

Addressing these research gaps will significantly enhance the understanding of private 5G network security. By focusing on vulnerabilities unique to private deployments, developing standardized protocols, and leveraging emerging technologies, future research can contribute to a more secure and robust foundation for private 5G networks. This will not only strengthen the security posture of these networks but also support their critical role in enabling next-generation applications and services across diverse sectors.

9.Conclusion

This SLR has thoroughly examined the security vulnerabilities in private 5G networks, addressing four critical research questions to guide the analysis. The findings provide a comprehensive understanding of the current state of security, identifying both advancements and significant gaps that must be addressed to ensure the resilience of private 5G networks. The review highlights a range of vulnerabilities unique to private 5G environments, including risks associated with network slicing, weak authentication mechanisms, edge computing challenges, and concerns over data privacy. These vulnerabilities necessitate specialized security measures tailored to the unique characteristics of private 5G deployments. The threats to the confidentiality, integrity, and availability (CIA) of data in private 5G networks are particularly pronounced due to their critical applications in industrial IoT, healthcare, and smart cities. Key threats include unauthorized access to sensitive data, man-in-the-middle attacks, data tampering, AI-driven system compromises, and denial-of-service (DoS) attacks. The high-stakes nature of these applications amplifies the consequences of security breaches, making robust mitigation strategies a priority.

In response to these threats, the review identifies several promising mitigation strategies, such as advanced encryption techniques, AI-based intrusion detection systems, and stronger authentication protocols like multi-factor authentication and blockchain-based identity management. However, challenges such as scalability, latency, and AI system vulnerabilities emphasise the need for further refinement of these solutions. The research also highlights critical gaps in the current body of literature. Notably, there is a lack of comprehensive security frameworks specifically tailored to private 5G networks. Many studies prioritize public 5G networks or focus on generalized 5G security, leaving private deployments inadequately addressed. Furthermore, there is a scarcity of experimental and case-based studies that assess the real-world effectiveness of proposed security measures.

In conclusion, the thesis emphasizes the importance of continued research into robust, scalable, and low-latency security frameworks specifically designed for private 5G networks. Future studies should also prioritize experimental evaluations to bridge the gap between theoretical solutions and practical implementation. As private 5G networks continue to proliferate, particularly in mission-critical industries, the need for secure, resilient networks has never been more urgent. This thesis lays a foundation for future research, advocating for an adaptive approach to securing private 5G networks against evolving threats and technological advancements.

References

Adebusola, J. A., Ariyo, A. A., Elisha, O. A., Olubunmi, A. M., & Julius, O. O. (2020). *An Overview of 5G Technology* 2020 International Conference in Mathematics, Ayobo, Nigeria. https://ieeexplore.ieee.org/document/9077620

Adil, M., Song, H., Khan, M. K., Farouk, A., & Jin, Z. (2024). 5G/6G-enabled metaverse technologies: Taxonomy, applications, and open security challenges with future research directions. https://doi.org/https://doi.org/10.1016/j.jnca.2024.103828

Ahad, A., Ali, Z., Mateen, A., Tahir, M., Hannan, A., Garcia, N. M., & Pires, I. M. (2023). A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions. *Volume 18*. https://doi.org/https://doi.org/10.1016/j.array.2023.100290

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). *5G security: Analysis of threats and solutions* 2017 IEEE Conference on Standards for Communications and Networking (CSCN, Helsinki, Finland. https://ieeexplore.ieee.org/abstract/document/8088621

Ahokangas, P., Matinmikko-Blue, M., Yrjölä, S., & Hämmäinen, H. (2021). Platform configurations for local and private 5G networks in complex industrial multi-stakeholder ecosystems. *ScienceDirect*, *Volume 45*(Issue 5). https://doi.org/https://doi.org/10.1016/j.telpol.2021.102128

Aijaz, A. (2020). Private 5G: The Future of Industrial Wireless. *vol. 14*(no. 4), pp. 136-145. https://doi.org/doi: 10.1109/MIE.2020.3004975

Alanazi, M. N. (2023). 5G Security Threat Landscape, AI and Blockchain. *Volume 133,*, 1467–1482 https://doi.org/https://doi.org/10.1007/s11277-023-10821-6

Altaleb, H., & Zoltán, R. (2023). *Addressing Cybersecurity Challenges in 5G-enabled IoT and Critical Infrastructures: A Comprehensive Overview* 2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES), Nairobi, Kenya. https://ieeexplore.ieee.org/document/10297774

Alwahaishi, S., & Zdrálek, J. (2020). *Biometric Authentication Security: An Overview* 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bengaluru, India. https://ieeexplore.ieee.org/abstract/document/9499970

Angin, P., Atalay, M., Gokce, F. C., & You, I. (2022). A Survey on the Security of European 5G Private Networks. *ResearchGate*. https://doi.org/DOI: 10.56801/rebicte.v8i.149

Badhwar, R. (2021). Man-in-the-Middle Attack Prevention. https://doi.org/Springer, Cham. https://doi.org/10.1007/978-3-030-75354-2_27 (Springer, Cham)

Bhandari, N., Devra, S., & Singh, K. (2017). Evolution of Cellular Network: From 1G to 5G *Volume 3*(Issue 5). https://d1wqtxts1xzle7.cloudfront.net/56615871/IJET-V3I5P23-libre.pdf?1526888401=&response-content-disposition=inline%3B+filename%3DEvolution_of_Cellular_Network_From_1G_to.pdf&Expires=1738994905&Signature=PbMuxhHWtt2x-sE~f-xqL59SlQnQluG-

aNkPsbNZ30k2I2aNSfUEVQ19uXEqhPZiqXUZCTDLVxxTpoNfvw~~uSsKyVz4SdCPIDOqJLH~15YlJct-uQLOMb3Jra4I0iLiVTxwhHcLResgSSHpxUJGd9eNAfRl4G9XP7ya78Uo3sWqsTZNdWLIyUbyDVGRjw8EXjF2qxXNLICALv-sohlqArRi3myJpQqoHk5-v9gUb~OdM6LIIY-E2yb4ub8S1UlzH-BH8qr1twL5b3ZP0AIlmRMmhE90ZR5qlKJ3jRMDT2e~oFrelxTcHR5F71oMziiD050y3Knk4vavP4gliO5wCw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Bhosale, K. S., Nenova, M., & Iliev, G. (2021). *A study of cyber attacks: In the healthcare sector* 2021 Sixth Junior Conference on Lighting (Lighting), Gabrovo, Bulgaria. https://ieeexplore.ieee.org/abstract/document/9598947

Chakraborty, P., Corici, M., Zope, H., Barjau, C., Awan, M. F., & Ribes, J. (2023). *A Framework for Roaming between 5G Non-Public-Networks (NPNs)* 2023 IEEE Conference on Standards for Communications and Networking (CSCN), Munich, Germany. https://ieeexplore.ieee.org/abstract/document/10453146

Chin, H.-H., Lin, H.-C., Cheng, Y.-C., & Tsai, C.-Y. (2023). Development status of 5G private networks in taiwan: law and practice. https://doi.org/https://doi.org/10.1007/s11276-023-03536-w

Corici, M., Chakraborty, P., Magedanz, T., Gomes, A. S., Cordeiro, L., & Mahmood, K. (2021). *5G Non-Public-Networks (NPN) Roaming Architecture* 2th International Conference on Network of the Future (NoF), Coimbra, Portugal. https://ieeexplore.ieee.org/document/9609936

Cui, Z., Cui, B., Su, L., Du, H., Xu, J., & Fu, J. (2024). A formal security analysis of the fast authentication procedure based on the security context in 5G networks. https://doi.org/https://doi.org/10.1007/s00500-023-09486-x

Djuitcheu, H., Mallikarjun, S. B., Habibi, M. A., Kuruvatti, N. P., & Schotten, H. D. (2023). *Securing Private 5G Campus Networks: Abstract Survey on Current Status, Security Threats, and Research Landscape* Conference on 6G Networking (6GNet), Paris, France. https://ieeexplore.ieee.org/document/10317752

Eluwole, O. T., Udoh, N., Ojo, M. O., & Okoro, C. (2018). From 1G to 5G, what next? *ResearchGate*. https://www.researchgate.net/publication/327527217_From_1G_to_5G_what_next

Eswaran, S., & Honnavalli, P. (2023). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Provided by the Springer Nature SharedIt content-sharing initiative*, *Volume 82*, pages 3–26, (2023). https://doi.org/https://doi.org/10.1007/s11235-022-00978-z

Ficzere, D., Soos, G., & Varga, P. (2021). *A compact 5G Non-Public Network* 2021 17th International Conference on Network and Service Management (CNSM), Izmir, Turkey. https://ieeexplore.ieee.org/document/9615528

Frank, H., Meixner, C. C., Assis, K. D. R., Yan, S., & Simeonidou, D. (2022). Techno-Economic Analysis of 5G Non-Public Network Architectures. *IEEE*, *10*, 1-1. https://doi.org/10.1109/ACCESS.2022.3187727

Gaber, T., Jazouli, Y. E., Eldesouky, E., & Ali, A. (2021). Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges. https://doi.org/https://doi.org/10.3390/electronics10111357

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., Abdel-Khalek, S., & Alkhassawneh, H. M. (2021). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. https://doi.org/ https://doi.org/10.1049/cmu2.12301

Javed, M. A., & Niazi, S. k. (2019). *5G Security Artifacts (DoS / DDoS and Authentication),* 2019 International Conference on Communication Technologies, Rawalpindi, Pakistan. https://ieeexplore.ieee.org/abstract/document/8737800

Ji, S., Garg, A. K., & Mishra, A. K. (2024). 5G Network Implementation: A Survey on Security Issues, Challenges, and Future Directions. pp. 62-88. https://doi.org/DOI: 10.4018/979-8-3693-5643-2.ch003

Karaagac, A., Dobrijevic, O., Schulz, D., Seres, G., Nazari, A., & Przybysz, H. (2023). *Managing 5G Non-Public Networks from Industrial Automation Systems* 2023 IEEE 19th International Conference on Factory Communication Systems (WFCS), Pavia, Italy. https://ieeexplore.ieee.org/document/10144248

Kim, W., Kim, K., Lee, J., & Park, H. (2023). 5G Architecture Based on Software-Defined Perimeter (SDP) for Direct Trust Access to Private Networks. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA*, pp. 2719-2721. https://doi.org/doi: 10.1109/CSCE60160.2023.00441

Kitchin, R., & Dodge, M. (2019). The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. https://doi.org/10.1080/10630732.2017.1408002

Lackner, T., Hermann, J., Dietrich, F., Kuhn, C., Angos, M., Jooste, J. L., & Palm, D. (2022). Measurement and comparison of data rate and time delay of end-devices in licensed sub-6 GHz 5G standalone non-public networks. *ScienceDirect*, *Volume 107*, Pages 1132-1137. https://doi.org/https://doi.org/10.1016/j.procir.2022.05.120

Lackner, T., Jooste, J. L., & Palm, D. (2023). Decision-support framework to evaluate the practicality of 5G for intralogistics use cases in standalone non-public networks. *Volume 120,*, Pages 51-56. https://doi.org/https://doi.org/10.1016/j.procir.2023.08.010

Lin, C.-C., Tsai, C.-T., Liu, Y.-L., Chang, T.-T., & Chang, Y.-S. (2023). Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges. *Volume 28*, pages 1043–1058. https://doi.org/https://doi.org/10.1007/s11036-023-02143-5

Liu, I.-H., Lee, M.-H., & Li, J.-S. (2023). Securing 5G Non-Public Networks Against Fake Base Station. *Journal of Robotics, Networking and Artificial Life*, *Vol. 10(2)*, pp. 156–159. https://www.jstage.jst.go.jp/article/jrnal/10/2/10_7/_pdf/-char/en

Maman, M., Calvanese-Strinati, E., Dinh, L. N., Haustein, T., Keusgen, W., Wittig, S., Schmieder, M., Barbarossa, S., Merluzzi, M., Costanzo, F., Sardellitti, S., Klessig, H., Kendre, S. V., Munaretto, D., Centenaro, M., Pietro, N. d., Liang, S.-P., Chih, K.-Y., Luo, J. S.-J., . . . Wang, T.-Y. (2021). Beyond private 5G networks: applications, architectures, operator models and technological enablers. *Spingerlink*. https://doi.org/https://doi.org/10.1186/s13638-021-02067-2

Mangla, C., Rani, S., Qureshi, N. M. F., & Singh, A. (2023). Mitigating 5G security challenges for next-gen industry using quantum computing [Journal]. *Volume 35*(6). https://www.sciencedirect.com/science/article/pii/S1319157822002373 (ScienceDirect)

Mazroa, A. A., & Arozullah, M. (2015). Securing the User Equipment (UE) in LTE Networks by Detecting Fake Base Stations *Volume-4*(Issue-6). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7122cc380c7997f0630497a67612f84b5f37cab8

Mejia, N. A., Perelló, J., Santos-Boada, G., & Amazonas, J. R. d. A. (2024). A Multidisciplinary Model to Quantify Human Uncertainty in Human-Centric Cyber-Physical-Social Systems: A 5G Application Use Case. *in IEEE Access*, *vol. 12*, pp. 63484-63503. https://doi.org/doi: 10.1109/ACCESS.2024.3396791

Mengist, W., Soromessa, T., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. *ScienceDirect*, *Volume 7, 2020, 100777*, Pages 134581. https://www.sciencedirect.com/science/article/pii/S221501611930353X

Mohan, J. P., Sugunaraj, N., & Ranganathan, P. (2022). *Cyber Security Threats for 5G Networks* 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA. https://ieeexplore.ieee.org/abstract/document/9813965

Nimkar, V. C., Pingle, S. A., & Bhagat, K. N. (2023). Private 5G, "Not As Private As You May Think". *ResearchGate*. https://doi.org/10.53555/jaz.v44iS8.3503

Ordóñez, J. A., Folgueira, J., Contreras, L. M., & Pastor, A. (2019). *The use of 5G Non-Public Networks to support Industry 4.0 scenarios* 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain. https://www.researchgate.net/publication/337703154_The_use_of_5G_Non-Public_Networks_to_support_Industry_40_scenarios

Pirayesh, H., & Zeng, H. (2022). Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE*, 767 - 809. https://doi.org/10.1109/COMST.2022.3159185

Prados-Garzon, J., Ameigeiras, P., Ordonez-Lucena, J., Muñoz, P., Adamuz-Hinojosa, O., & Camps-Mur, D. (2021). 5G Non-Public Networks: Standardization, Architectures and Challenges. *IEEE Access*, *vol. 9*, pp. 153893-153908. https://doi.org/doi: 10.1109/ACCESS.2021.3127482.

Purification, S., Wuthier, S., Kim, J., Kim, J., & Chang, S.-Y. (2024). *Fake Base Station Detection and Blacklisting* 2024 33rd International Conference on Computer Communications and Networks (ICCCN), Kailua-Kona, HI, USA. https://ieeexplore.ieee.org/abstract/document/10637542

Ramezanpour, K., Jagannath, J., & Jagannath, A. (2023). Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. *ScienceDirect*, *Volume 221*. https://doi.org/https://doi.org/10.1016/j.comnet.2022.109515

Rostamia, A., Patelb, D., Giyyarpuramc, M., & Pedersena, F. (2023). 5G Non-Public Network for Industrial IoT: Operation Models. https://doi.org/DOI:10.48550/arXiv.2307.10781

Sarakis, L., trakadas, P., Martrat, J., Prior, S., Trullols-Cruces, O., Coronado, E., Centenaro, M., Kontopoulos, G., Atxutegi, E., Gkonis, P. k., Gonzalez-Diaz, S., Antonopoulos, A., Siddiqui, S., & Merino, P. P. (2021). Cost-Efficient 5G Non-Public Network Roll-Out: The Affordable5G Approach. *IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece,*, pp. 221-227. https://doi.org/doi: 10.1109/MeditCom49071.2021.9647555

Shukurillaevich, U. B., Sattorivich, R. O., & Amrillojonovich, R. U. (2019). *5g Technology Evolution," 2019 International Conference on Information Science and Communications Technologies (ICISCT)* Tashkent, Uzbekistan. https://ieeexplore.ieee.org/document/9011957

Suraci;, C., Giuseppe Araniti, Andrea Abrardo, Guiseppe Bianchi, & Antonio Lera. (2021). A stakeholder-oriented security analysis in virtualized 5G cellular networks. *ScienceDirect*, *Volume 184,*(107604). https://doi.org/https://doi.org/10.1016/j.comnet.2020.107604.

Tripathi, A., Thakur, A., & Tamma, B. R. (2022). *Attack Graphs for Standalone Non-Public 5G Networks* Montreal, QC, Canada. https://ieeexplore.ieee.org/document/10056670

V, P. G., Meeradevi, & V, S. (2022). *Survey on Security Risks in 5G Private Industrial Networks* Bangalore, India. https://ieeexplore.ieee.org/document/10057943

Vij, S., & Jain, A. (2016). *5G: Evolution of a secure mobile technology* 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India. https://ieeexplore.ieee.org/document/7724653

Wani, M., Horstmann, T., & Kretschmer, M. (2024). Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. *4*, 23-40. https://doi.org/https://doi.org/10.3390/jcp4010002

Wen, M., Li, Q., Kim, K. J., Lopez-Perez, D., Dobre, O. A., & Poor, H. V. (2022). Private 5G Networks: Concepts, Architectures, and Research Landscape. *IEEE*, *16*(1 January 2022), 7-25. https://doi.org/10.1109/JSTSP.2021.3137669

Appendix

Appendix A: List of studies included in SLR

Published Date (year)	Title	Author(s)	Database
2015	Securing the User Equipment (UE) in LTE Networks by Detecting Fake Base Stations	Alanoud Al Mazroa, Mohammed Arozullah	International Journal of Soft Computing and Engineering (IJSCE)
2016	Compromises in Healthcare Privacy due to Data Breaches	S. Srinivasan	European Scientific Journal
2016	5G: Evolution of a secure mobile technology	Sonakshi Vij, Amita Jain	IEEE
2017	5G security: Analysis of threats and solutions	Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov	IEEE
2017	Evolution of Cellular Network: From 1G to 5G	Nikhil Bhandari, Shivinder Devra, Karamdeep Singh	Academia
2018	From 1G to 5G, what next?	O. T. Eluwole, Nsikak Udoh, Mike Oluwatayo Ojo, Cindy Okoro	ResearchGate
2019	5G Security Artifacts (DoS / DDoS and Authentication)	M Awais Javed Sohaib khan Niazi	IEEE
2019	The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention	Rob Kitchin Martin Dodge	ResearchGate
2019	The use of 5G Non-Public Networks to support Industry 4.0 scenarios	José Antonio Ordóñez, Jesus Folgueira, Luis M. Contreras, Antonio Pastor	IEEE
2019	5g Technology Evolution," 2019 International Conference on Information Science and Communications Technologies (ICISCT)	Usmonov Botir Shukurillaevich, Radjabov Ozod Sattorivich, Rustamov Umedjon Amrillojonovich	IEEE
2020	An Overview of 5G Technology	Joyce Ayoola Adebusola, Adebiyi Ayodele Ariyo, Okeyinka Aderemi Elisha, Adebiyi Marion Olubunmi, Okesola Olatunji Julius	IEEE
2020	Private 5G: The Future of Industrial Wireless	Adnan Aijaz	IEEE

2020	Biometric Authentication Security: An Overview	Saleh Alwahaishi, Jaroslav Zdrálek	IEEE
2020	Method for conducting systematic literature review and meta-analysis for environmental science research	Wondimagegn Mengist, Teshome Soromessa, Gudina Legese	ScienceDirect
2021	Platform configurations for local and private 5G networks in complex industrial multi-stakeholder ecosystems	Petri Ahokangas Marja Matinmikko-Blue Seppo Yrjölä Heikki Hämmäinen	ScienceDirect
2021	Man-in-the-Middle Attack Prevention	Raj Badhwar	Springer
2021	A study of cyber attacks: In the healthcare sector	Karuna S Bhosale, Maria Nenova, Georgi Iliev	IEEE
2021	5G Non-Public-Networks (NPN) Roaming Architecture	Marius Corici Pousali Chakraborty Thomas Magedanz Andre S. Gomes Luis Cordeiro Kashif Mahmood	IEEE
2021	A compact 5G Non-Public Network	Daniel Ficzere, Gabor Soos, Pal Varga	IEEE
2021	Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges	Tarek Gaber, Yassine El Jazouli, Esraa Eldesouky, Ahmed Ali	MDPI
2021	A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things	Mohammad Kamrul Hasan, Taher M. Ghazal, Rashid A. Saeed, Bishwajeet Pandey, Hardik Gohel, Ala' A. Eshmawi, S. Abdel-Khalek, Hula Mahmoud Alkhassawneh	IET Research
2021	An impact of implementation of 5G Technology	Dražen Lučić, Petar Mišević	IEEE
2021	Beyond private 5G networks: applications, architectures, operator models and technological enablers	Mickael Maman, Emilio Calvanese-Strinati, Lam Ngoc Dinh, Thomas Haustein, Wilhelm Keusgen, Sven Wittig, Mathis Schmieder, Sergio Barbarossa, Mattia Merluzzi, Francesca Costanzo,	SpringerLink

		Stefania Sardellitti, Henrik Klessig, Savita Vitthalrao Kendre, Daniele Munaretto, Marco Centenaro, Nicola di Pietro, Shuo-Peng Liang, Kuan-Yi Chih, Jack Shi-Jie Luo, Ling-Chih Kao, Jiun-Cheng Huang, Jen-Sheng Huang, Tzu-Ya Wang	
2021	Cost-Efficient 5G Non-Public Network Roll-Out: The Affordable5G Approach	Lambros Sarakis Panagiotis trakadas Josep Martrat Simon Prior Oscar Trullols-Cruces Estefania Coronado Marco Centenaro G. Kontopoulos Eneko Atxutegi Panagiotis k. Gkonis S. Gonzalez-Diaz Angelos Antonopoulos Shuaib Siddiqui Pedro Plaza Merino	IEEE
2021	A stakeholder-oriented security analysis in virtualized 5G cellular networks	Chiara Suraci; Giuseppe Araniti, Andrea Abrardo, Guiseppe Bianchi, Antonio Lera,	ScienceDirect
2022	A Survey on the Security of European 5G Private Networks	Pelin Angin, Manolya Atalay, Fatma Ceyda Gokce, Ilsun You	ResearchGate
2022	Techno-Economic Analysis of 5G Non-Public Network Architectures	Hilary Frank Carlos Colman Meixner K.D.R. Assis Shuangyi Yan Dimitra Simeonidou	IEEE
2022	Measurement and comparison of data rate and time delay of end-devices in licensed sub-6 GHz 5G standalone non-public networks	Thorge Lackner, Julian Hermann, Fabian Dietrich, Christian Kuhn, Mario Angos, Johannes L. Jooste, Daniel Palm	ScienceDirect
2022	Cyber Security Threats for 5G Networks	Jaya Preethi Mohan, Niroop Sugunaraj, Prakash Ranganathan	IEEE

2022	Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey	Hossein Pirayesh, Huacheng Zeng	
2022	Attack Graphs for Standalone Non-Public 5G Networks	Arpit Tripathi, Abhishek Thakur, Bheemarjuna Reddy Tamma	IEEE
2022	Survey on Security Risks in 5G Private Industrial Networks	Pavan G V, Meeradevi, Sangeetha V	IEEE
2022	Private 5G Networks: Concepts, Architectures, and Research Landscape	Miaowen Wen, Qiang Li, Kyeong Jin Kim, David Lopez-Perez, Octavia A. Dobre, H. Vincent Poor	IEEE
2023	A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions	Abdul Ahad, Zahra Ali , Abdul Mateen, Mohammad Tahir, Abdul Hannan , Nuno M. Garcia, Ivan Miguel Pires	ScienceDirect
2023	5G Security Threat Landscape, AI and Blockchain	Mohammad N. Alanazi	Springer
2023	Addressing Cybersecurity Challenges in 5G-enabled IoT and Critical Infrastructures: A Comprehensive Overview	Haya Altaleb, Rajnai Zoltán	IEEE
2023	A Framework for Roaming between 5G Non-Public-Networks (NPNs)	Pousali Chakraborty, Marius Corici, Hemant Zope, Carlos Barjau, Muhammad Faheem Awan, Josep Ribes	IEEE
2023	Development status of 5G private networks in taiwan: law and practice.	Hui-Hsin Chin, Hao-Chu Lin, Yi-Chu Cheng, Chung-Yi Tsai	Springer
2023	Securing Private 5G Campus Networks: Abstract Survey on Current Status, Security Threats, and Research Landscape	Hubert Djuitcheu, Sachinkumar Bavikatti, Mallikarjun Mohammad Asif Habibi Nandish P. Kuruvatti Hans D. Schotten	IEEE
2023	Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions.	Sivaraman Eswaran Prasad Honnavalli	Springer
2023	Managing 5G Non-Public Networks from Industrial Automation Systems	Abdulkadir Karaagac Ognjen Dobrijevic Dirk Schulz Gergely Seres	IEEE

		Ala Nazari Hubert Przybysz	
2023	5G Architecture Based on Software-Defined Perimeter (SDP) for Direct Trust Access to Private Networks	Woocheol Kim, Kiwon Kim, Jongkuk Lee, HeaSook Park	ResearchGate
2023	Decision-support framework to evaluate the practicality of 5G for intralogistics use cases in standalone non-public networks	Thorge Lackner, Johannes L. Jooste, Daniel Palm	ScienceDirect
2023	Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges	Chun-Cheng Lin Ching-Tsorng Tsai Yu-Liang Liu Tsai-Ting Chang Yung-Sheng Chang	Springer
2023	Securing 5G Non-Public Networks Against Fake Base Station	I-Hsien Liu, Meng-Huan Lee, Jung-Shian Li	Jstage
2023	Mitigating 5G security challenges for next-gen industry using quantum computing	Cherry Mangla, Shalli Rani, Nawab Muhammad Faseeh Qureshi, Aman Singh	ScienceDirect
2023	Three Deployment Models for Private 5G Network	IPLOOK Networks	IPLOOK Networks
2023	Private 5G, “Not As Private As You May Think”	V. C. Nimkar, S. A. Pingle, K. N. Bhagat	ResearchGate
2023	Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective	Keyvan Ramezanpour, Jithin Jagannath, Anu Jagannath	ScienceDirect
2023	5G Non-Public Network for Industrial IoT: Operation Models	Ahmad Rostamia Dhruvin Patelb Madhusudan Giyyarpuramc Finn Pedersena	ResearchGate
2024	5G/6G-enabled metaverse technologies: Taxonomy, applications, and open security challenges with future research directions	Muhammad Adil, Houbing Song, Muhammad Khurram Khan, Ahmed Farouk, Zhanpeng Jin	ScienceDirect
2024	A formal security analysis of the fast authentication procedure based on the security context in 5G networks	Zhiwei Cui, Baojiang Cui, Li Su, Haitao Du, Jie Xu, Junsong Fu	Springer
2024	5G Network Implementation: A Survey on Security Issues,	Sharma Ji, Ajay Kumar Garg, Abhishek Kumar Mishra	IgI Global

	Challenges, and Future Directions		
2024	A Multidisciplinary Model to Quantify Human Uncertainty in Human-Centric Cyber-Physical-Social Systems: A 5G Application Use Case	Nestor Alzate Mejia, Jordi Perelló, Germán Santos-Boada, José Roberto de Almeida Amazonas	IEEE
2024	Fake Base Station Detection and Blacklisting	Sourav Purification, Simeon Wuthier, Jinoh Kim, Jonghyun Kim, Sang-Yoon Chang	IEEE
2024	Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy	Mohamad Wani Thorsten Horstmann Mathias Kretschmer	MDPI