INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO
ESTG

SECURITY CHALLENGES IN 5G NETWORK SLICING: A THEORETICAL ANALYSIS AND FRAMEWORK PROPOSAL

José Carlos Gomes Lopes Dias

Escola Superior de Tecnologia e Gestão

SECURITY CHALLENGES IN 5G NETWORK SLICING: A THEORETICAL ANALYSIS AND FRAMEWORK PROPOSAL
José Carlos Gomes Lopes Dias

2025

INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

José Carlos Gomes Lopes Dias

SECURITY CHALLENGES IN 5G NETWORK SLICING: A THEORETICAL ANALYSIS AND FRAMEWORK PROPOSAL

Mestrado em Cibersegurança

Trabalho efetuado sob a orientação do(s)
Professor(a) Doutor(a) Silvestre Malta
Professor(a) Doutor(a) Ricardo Santos

Janeiro de 2025

Instituto Politécnico
de Viana do Castelo

Security Challenges in 5G Network Slicing: A Theoretical Analysis and Framework Proposal

Autor(a)

José Carlos Dias

Trabalho orientado por

Professor Silvestre Malta e Professor Ricardo Santos

Mestrado em Cibersegurança

20 de 09 de 2025

Mestrado em Cibersegurança
Master in Cybersecurity

Security Challenges in 5G Network Slicing: A Theoretical Analysis and Framework Proposal

a master's thesis authored by

Jose Carlos Gomes Lopes Dias

and supervised by

Silvestre Malta
Professor Adjunto Convidado, ESTG-IPVC

Ricardo Santos
Professor Coordenador, ESTG-IPP

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

23 de março de 2026

Abstract

Abstract

This dissertation analyses the security challenges associated with network slicing in 5th Generation (5G) architectures, with a particular focus on how vulnerabilities across the orchestration, virtualisation, and communication layers can undermine isolation guarantees. Although network slicing enables flexible multi-tenant services, the sharing of resources and the presence of complex interdependencies broaden the attack surface. Exploratory tests conducted using open-source platforms such as Free5GC, Open Source MANO (OSM), and User Equipment Radio Access Network Simulator (UERANSIM) revealed significant limitations in terms of maturity and compatibility, highlighting the gap between theoretical models and practical implementations.

To address this issue, a structured taxonomy of vulnerabilities was developed to classify security weaknesses across the different layers of the network slicing system and to analyse them through representative attack scenarios. Building on this analysis, a conceptual security framework is proposed, integrating preventive, monitoring, and automated response mechanisms to strengthen slice isolation and resilience. The framework emphasises adaptive security through continuous monitoring and dynamic policy enforcement, thereby contributing to the secure design of future 5G and beyond-5G networks.

Keywords: 5G networks. network slicing. vulnerabilities. security. risk mitigation.

Resumo

Resumo

Esta dissertação analisa os desafios de segurança associados ao network slicing em arquiteturas 5G, com particular enfoque em como vulnerabilidades nas camadas de orquestração, virtualização e comunicação podem comprometer as garantias de isolamento. Embora o network slicing permita serviços multi-tenant flexíveis, a partilha de recursos e a presença de interdependências complexas alargam a superfície de ataque. Testes exploratórios realizados com plataformas open source como Free5GC, OSM e UERANSIM revelaram limitações significativas em termos de maturidade e compatibilidade, evidenciando o desfasamento entre os modelos teóricos e as implementações práticas.

Para responder a esta problemática, foi desenvolvida uma taxonomia estruturada de vulnerabilidades para classificar fraquezas de segurança nas diferentes camadas do sistema de network slicing e analisá-las através de nove cenários de ataque representativos. Com base nesta análise, é proposto um enquadramento conceptual de segurança que integra mecanismos preventivos, de monitorização e de resposta automatizada para reforçar o isolamento e a resiliência das slices. O modelo enfatiza uma segurança adaptativa, baseada em monitorização contínua e aplicação dinâmica de políticas, contribuindo para o desenho seguro de redes 5G e de e de futuras gerações.

Palavras-chave: 5G networks. network slicing. vulnerabilities. security. risk mitigation.

Aknowledgements

I would like to express my deepest gratitude to my supervisor, Professor Silvestre Malta and Professor Ricardo Santos, for their invaluable guidance, insightful feedback, and continuous support throughout this dissertation. Their expertise and patience were fundamental in shaping both the direction and quality of this work.

I am also thankful to the academic staff and colleagues at Escola Superior de Tecnologia e Gestão (ESTG), whose discussions and suggestions enriched this dissertation. Special thanks go to my teammates and friends for their encouragement and for creating a collaborative and motivating environment.

I gratefully acknowledge G9Telecom for providing the resources and infrastructure that made this dissertation possible.

Finally, I would like to thank my family for their unconditional support, understanding, and encouragement throughout this journey. Their patience and belief in me have been an endless source of motivation.

Contents

List of Figures

List of Tables

List of Abbreviations

(R)AN (Radio) Access Network

3GPP 3rd Generation Partnership Project

3GPP SA5 3rd Generation Partnership Project Service and System Aspects Working Group 5

4G Fourth Generation

5G 5th Generation

6G Sixth Generation

ACL Access Control List

ACM Association for Computing Machinery

AF Application Function

AI Artificial Intelligence

AMF Access and Mobility Management Function

API Application Programming Interface

AR Augmented Reality

AUSF Authentication Server Function

B5G Beyond 5G

C-RAN cloud-based radio access networks

CIA Confidentiality, Integrity, and Availability

CNF Cloud-Native Network Function

CPU Central Processing Unit

CSIRT Computer Security Incident Response Team

CVE Common vulnerabilities and Exposures

D2D device-to-device

DDoS Distributed Denial of Service

DN Data Network

DoS Denial of Service

DRL Deep Reinforcement Learning

eMBB enhanced Mobile Broadband

ENISA European Union Agency for Cybersecurity

ESTG Escola Superior de Tecnologia e Gestão

ETSI European Telecommunications Standards Institute

EU European Union

Gbps Gigabits per second

GDPR General Data Protection Regulation

gNB Next Generation NodeB

GSM Global System for Mobile Communications

HD high-definition

HTTP Hypertext Transfer Protocol

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IoT Internet of Things

IP Internet Protocol

ISO International Organization for Standardization

ISO/IEC International Organization for Standardization/International Electrotechnical Commission

KVM Kernel-based Virtual Machine

LTE Long Term Evolution

LTS Long-Term Support

M-MIMO massive MIMO

M2M machine-to-machine

MANO Management and Orchestration

MCyber Master in Cybersecurity

MEC Multi-access Edge Computing

MitM Man-in-the-Middle

ML Marchine Learning

mMTC massive Machine-Type Communications

MPDI Multidisciplinary Digital Publishing Institute

ms milliseconds

MTTD Mean Time to Detect

MTTR Mean Time to Respond

NEF Network Exposure Function

NF Network Function

NFV Network Functions Virtualization

NIS Network and Information Security

NIS2 Network and Information Security Directive 2 (EU 2022/2555)

NIST National Institute of Standards and Technology

NOMA Non-Orthogonal Multiple Access

NR New Radio

NRF Network Repository Function

NS Network Service

NSD Network Service Descriptor

NSMF Network Slice Management Function

NSSF Network Slice Selection Function

NSSMF Network Slice Subnet Management Function

OAI Open Air interface

OMA Orthogonal Multiple Access

ONAP Open Network Automation Platform

OSM Open Source MANO

OWASP Open Worldwide Application Security Project

PCF Policy Control Function

PDU Protocol Data Unit

QEMU Quick Emulator

QoS Quality of Service

RAM Random Access Memory

RBAC Role-Based Access Control

RSMA Rate Splitting Multiple Access

S-NSSAI Single Network Slice Selection Assistance Information

SBA Service-Based Architecture

SDN Software Defined Networking

SIEM Security Information and Event Management

SLA Service Level Agreement

SMF Session Management Function

SMS Short Message Service

SOC Security Operations Center

SSID Service Set Identifiers

STIX Structured Threat Information Expression

TAXII Trusted Automated Exchange of Intelligence Information

THz Terahertz

TLS Transport Layer Security

UDM Unified Data Management

UE User Equipment

UERANSIM User Equipment Radio Access Network Simulator

UMTS Universal Mobile Telecommunications System

UPF User Plane Function

URLLC Ultra-Reliable Low-Latency Communications

vCPU Virtual Central Processing Unit

VLAN Virtual Local Area Network

VM Virtual Machine

VNF Virtualized Network Functions

VNFD Virtualized Network Function Descriptors

VR Virtual Reality

VXLAN Virtual Extensible Local Area Network

WCDMA Wideband Code Division Multiple Access

WN Wireless Network

XR Extended Reality

YAML Yet Another Markup Language

ZAP Zed Attack Proxy

ZTNA Zero Trust Network Access

Chapter 1

Introduction

The growing complexity and critical role of mobile communications in modern society demand not only faster and more flexible networks, but also a rethinking of how these networks are designed, deployed, and secured. This need has led to the emergence of fifth-generation mobile networks, which introduce a range of architectural and operational innovations [43]. Among these, network slicing stands out as a paradigm shift with far-reaching implications for both service delivery and security. This chapter provides the necessary context for understanding the scope of this dissertation, outlines the problem it addresses, presents the research objectives and contributions, and describes the overall structure of the document.

1.1 Context

The evolution towards 5th Generation (5G) mobile networks [8] has introduced fundamental architectural changes aimed at addressing the growing demand for high-performance, low-latency, and flexible communication services. One of the most disruptive innovations brought by 5G is network slicing, which allows multiple isolated virtual networks to be created on top of a shared physical infrastructure. These slices can be tailored to meet the specific requirements of diverse use cases, such as autonomous vehicles, smart cities, and industrial Internet of Things (IoT) [6] [3]. While network slicing introduces unprecedented flexibility and scalability, it also increases the potential attack surface and poses new challenges in terms of security, isolation, and trust management [5].

1.2 Problem Statement and Motivation

Although the research community has widely recognized the theoretical security risks associated with network slicing, including inter-slice attacks, resource leakage, and compromised management interfaces, practical implementations and empirical evaluations remain scarce[1]. Initial efforts to reproduce and simulate realistic 5G slicing environments using open-source tools such as Free5GC[1], Open Source MANO (OSM)[2], and User Equipment Radio Access Network Simulator (UERANSIM)[3] have revealed significant limitations: lack of maturity, version incompatibilities, unstable orchestration environments, and insufficient support for dynamic slice instantiation and isolation mechanisms. These aspects will be further detailed in Chapter 3.

These constraints posed a methodological challenge: the original experimental approach, which focused on simulating and executing security attacks in controlled test environments, proved technically infeasible given the limitations of the available tools and resources. Nevertheless, rather than discarding these limitations as mere obstacles, this dissertation reframes them as empirical data, supporting a theoretical and critical analysis of the current state of 5G network slicing security.

1.3 Objectives

The initial goal of this thesis was to investigate and ensure the isolation and security of network slicing, specifically at the network layer of 5G systems. This was to be achieved through a series of experimental steps, including:

- Identifying and testing specific vulnerabilities in slice isolation at the network layer;
- Simulating attacks in multi-slice scenarios to assess their impact on network performance and security;
- Developing and validating dynamic mitigation solutions, such as firewall policies and resource allocation mechanisms;

[1] https://www.free5gc.org/
[2] https://osm.etsi.org/
[3] https://github.com/aligungr/UERANSIM

- Proposing a framework of best practices aimed at improving isolation in real-world environments.

However, as detailed in Chapter 3, exploratory experiments conducted with open-source 5G platforms, particularly Open Source MANO (OSM) and Free5GC, revealed practical limitations that affected the feasibility of the initial experimental plan. More specifically, issues related to orchestration, platform instability, and limited tool maturity hindered the creation of reliable multi-slice environments and prevented the realistic implementation of attack scenarios within the available scope.

Therefore, the objectives of this dissertation were reformulated to focus on a theoretical and analytical approach, while still pursuing the overarching goal of improving the understanding and security of network slicing. The revised objectives are:

- To critically assess the state of the art in 5G network slicing security, with a focus on isolation mechanisms;
- To document and analyse the technical limitations of current open-source tools through a structured experimental methodology;
- To propose a theoretical framework for improving slice isolation, incorporating monitoring and automated response mechanisms;
- To develop a taxonomy of vulnerabilities and tool constraints relevant to slicing security;
- To provide practical recommendations and guidelines for future research and secure implementation of 5G slicing architectures.

1.4 Contributions

This work makes the following original contributions:

- A systematic documentation of technical obstacles encountered when deploying open-source 5G slicing environments, offering empirical insight into their limitations;

- A detailed analysis of vulnerabilities based on current literature and structured through a domain-specific taxonomy;
- The proposal of a theoretical security framework for network slicing, addressing isolation, orchestration, and detection/response mechanisms;
- A set of practical recommendations and guidelines for researchers and developers aiming to evaluate or enhance the security of network slicing systems.

The research outcomes of this thesis have also led to peer-reviewed scientific publications:

- 5G Network Slicing: Security Challenges, Attack Vectors, and Mitigation Approaches
  - Publisher: Sensors - MDPI;
  - Publish Date: 24 June 2025;
  - DOI: doi.org/10.3390/s25133940.
- Security Challenges in 5G Network Slicing: A Risk-Based Analysis and Conceptual Framework
  - Publisher: Journal of Cybersecurity and Privacy - MPDI;
  - Publish Date: 12 February 2026;
  - DOI: doi.org/10.3390/jcp6010035.

1.5 Organization

This dissertation is structured into seven chapters. Following this introductory chapter, Chapter 2 provides a comprehensive review of the state of the art in 5G network slicing, with a particular focus on security challenges and vulnerabilities documented in the literature. It also includes a critical analysis of existing open-source tools, exposing the disconnect between theoretical models and their practical implementation. Chapter 3 presents the research methodology adopted in this work, beginning with the initial experimental approach and detailing the technical challenges encountered during tool deployment. These difficulties are subsequently reframed as valid research data, justifying the transition to a

theoretical and analytical perspective. Chapter 4 offers an in-depth theoretical analysis of the vulnerabilities associated with network slicing, structured around a domain-specific taxonomy. Building on this analysis, Chapter 5 proposes a theoretical framework for enhancing the security of 5G network slicing, integrating principles of isolation, monitoring, and automated response. Chapter 6 consolidates the main findings with an interpretation of the conceptual framework and a comparison with the findings identified on the State-of-the-Art. Finally, Chapter 7 concludes the dissertation by summarizing the contributions of the study and outlining directions for future research, particularly as simulation and orchestration tools mature and enable more realistic and scalable experimentation.

Chapter 2

State-of-the-Art and Critical Analysis

This chapter begins by introducing the fundamental concepts underlying 5G networks and network slicing, establishing the architectural and operational context required for the subsequent evaluation of experimental tools. Building on this foundation, the chapter then provides a critical analysis of open-source platforms used to experiment with 5G network slicing. The goal is to assess their suitability for security-related research, particularly with regard to slice isolation and orchestration. The tools examined include orchestrators, 5G core implementations, and simulation or emulation frameworks. The analysis reflects direct experimentation, configuration efforts, and an examination of available documentation and community support. Emphasis is placed on identifying technical limitations, architectural constraints, and security shortcomings that have shaped the methodological decisions presented in the following chapter.

2.1 Foundations of 5G Networks and Network Slicing

The rapid evolution of mobile communications has culminated in the emergence of 5G, a generation defined not only by enhanced performance but also by a fundamental shift in architectural principles. Understanding these underlying concepts is essential for analysing the security challenges associated with network slicing, a key innovation that enables the creation of tailored virtual networks over shared physical infrastructure. This section

provides the technical groundwork required for the subsequent chapters by outlining the evolution of mobile networks, the architectural structure of 5G systems, the operational models that motivate differentiated service requirements, and the core principles behind network slicing. Together, these foundations establish the context necessary to assess the security implications explored later in this dissertation.

2.1.1 Evolution of Mobile Networks

The development of mobile communication systems has progressed through successive generations, each introducing technological and architectural improvements that have shaped the landscape of today's connectivity. Early generations prioritized basic voice services, while later iterations expanded capabilities to support mobile data, broadband access, and fully IP-based communication [13]. This progression culminates in 5G, which departs from traditional monolithic architectures by adopting virtualisation, software-defined networking, and native cloud principles. These structural changes lay the foundation for advanced service differentiation and dynamic orchestration mechanisms, ultimately enabling concepts such as network slicing [44] [28]. Table 2.1 summarizes the main characteristics of each generation and the associated technological milestones.

The transition from static, hardware-centric infrastructures to programmable, service-oriented architectures is therefore a key enabler of 5G capabilities. In particular, the combination of virtualised core functions, flexible resource allocation, and support for diverse performance requirements creates the conditions under which multiple logical networks can coexist over a shared physical substrate. This evolution directly motivates the emergence of network slicing, which capitalises on these architectural principles to deliver customised and isolated service environments.

2.1.2 5G System Architecture

The 5G system introduces a service-based and cloud-native architecture designed to support highly flexible, scalable, and programmable network deployments. Unlike previous generations, which relied on monolithic core components and hardware-centric designs, the 5G Core adopts a modular structure organised into distinct control and user planes. This separation enables independent scaling, optimised resource allocation, and the creation of

Table 2.1: Evolution of mobile network generations

Gen.	**Year**	**Technology**	**Characteristics**	**Use Cases**
1G	1980s	Analog Voice	Analog voice; low quality	Basic calls
2G	1990s	Global System for Mobile Communications (GSM)	Digital voice; Short Message Service (SMS); better security	Calls, SMS
3G	2000s	Universal Mobile Telecommunications System (UMTS)/Wideband Code Division Multiple Access (WCDMA)	Mobile data; early internet	Browsing, media
4G	2010s	Long Term Evolution (LTE)	High-speed data; all-Internet Protocol (IP)	Streaming, apps
5G	2020s	New Radio (NR), Virtual Core	Ultra-low latency; high capacity; massive IoT	IoT, Augmented Reality (AR)/Virtual Reality (VR), autonomous systems
6G	2030s	Terahertz (THz), Artificial Intelligence (AI)-Native	Sub-ms latency; Tbps speeds	Extended Reality (XR), AI systems

customised service environments [35] [17] [31]. Figure 2.1 provides a high-level overview of the main functional elements of the 5G system and the interfaces that interconnect them.

In the control plane, the Service-Based Architecture enables network functions to communicate through standardised Application Programming Interfaces (APIs) rather than fixed signalling paths. Core entities such as the Access and Mobility Management Function (AMF), Session Management Function (SMF), Authentication Server Function (AUSF), Unified Data Management (UDM), Policy Control Function (PCF), Network Repository Function (NRF), Network Slice Selection Function (NSSF) and Network Exposure Function (NEF) coordinate authentication, mobility, policy enforcement and slice selection through service-based interfaces. This modular design improves flexibility and facilitates orchestration mechanisms essential for dynamic slice management.

The user plane is centred on the User Plane Function (UPF), responsible for forwarding traffic between the (Radio) Access Network ((R)AN) and external Data Networks.

Interfaces such as N3, N4 and N6 support distributed deployments, allowing operators to optimise routing, reduce latency and integrate edge-computing solutions.

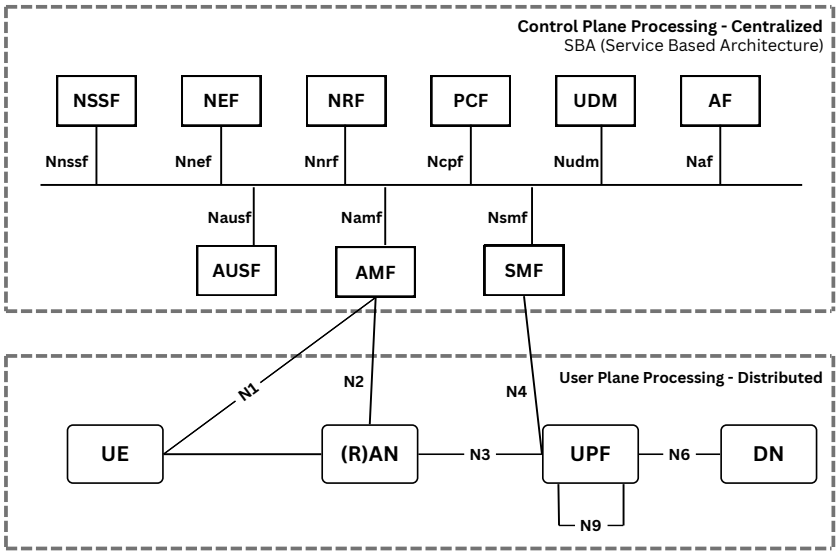

Figure 2.1: 5G system architecture

Together, the Service-Based Architecture (SBA) control plane and the distributed user plane form the programmable architecture that enables differentiated service paths and the isolation capabilities required for network slicing, providing the operational basis for the topics discussed in the subsequent subsections.

2.1.3 5G Service Categories

The 5G system supports diverse application requirements through three primary service categories defined by 3rd Generation Partnership Project (3GPP) [10]. These categories enable differentiated performance levels and form the basis for the customisable service behaviour that network slicing provides [33]. Figure 2.2 illustrates the operational modes and typical application scenarios.

The three categories are:

- **enhanced Mobile Broadband (eMBB)** — high data rates and sustained throughput for bandwidth-intensive applications such as high-definition (HD)/4K streaming, cloud services and immersive multimedia [22];
- **Ultra-Reliable Low-Latency Communications (URLLC)** — extremely low latency and high reliability for mission-critical services, including autonomous vehicles,

industrial automation and remote control systems [36] [15];

- **massive Machine-Type Communications (mMTC)** — scalable and energy-efficient connectivity for a high number of IoT devices, suitable for smart cities [4], sensor networks and large-scale monitoring [32].

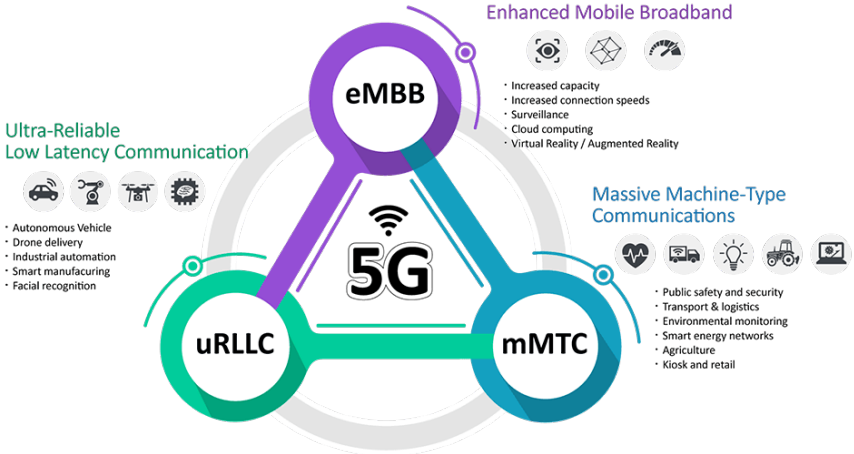

Figure 2.2: Main 5G service categories and their application scenarios

These categories impose distinct performance requirements, compelling 5G networks to support multiple service profiles simultaneously. This diversity reinforces the need for programmable and isolated virtual environments, a capability realised through network slicing.

2.1.4 Fundamentals of Network Slicing

Network slicing is a core capability of 5G, enabling the creation of multiple virtual networks over a shared physical infrastructure. Each slice functions as an isolated logical environment, configured with its own performance, reliability and security attributes, allowing the network to adapt to distinct service requirements [19] [34] [40].

From an architectural perspective, slicing extends across three functional planes. The data plane is responsible for forwarding user traffic and enforcing slice-specific Quality of Service (QoS) policies [16] [25]. The control plane manages signalling, session configuration and the association of devices with the appropriate slice. The management plane oversees lifecycle operations such as creation, scaling, modification and termination of slices [2].

Together, these planes provide the logical separation and resource independence needed to support diverse services.

The implementation of slicing is supported by several enabling technologies:

- Software Defined Networking (SDN), which centralises control and separates control and data planes [21];
- Network Functions Virtualization (NFV), which replaces hardware appliances with virtualised or cloud-native network functions [18];
- Orchestration frameworks such as European Telecommunications Standards Institute (ETSI) MANO, Network Slice Management Function (NSMF) and Network Slice Subnet Management Function (NSSMF), which automate the provisioning and coordination of slice resources across the system.

These elements collectively provide the programmable and flexible substrate required to deploy customised and isolated network slices, establishing the foundation for the security considerations explored in the next subsection.

2.1.5 Isolation Requirements and Early Security Considerations

The ability to host multiple virtual networks over a shared physical infrastructure makes isolation a fundamental requirement in 5G network slicing. Effective separation must be ensured at different levels: logical isolation, to prevent cross-slice access or signalling interference; functional isolation, guaranteeing that control and user plane operations remain independent across slices; and resource isolation, ensuring that compute, storage and bandwidth allocations are not inadvertently shared or influenced by other slices.

These requirements become more complex in environments characterised by virtualisation and multi-tenancy [42]. Since network functions may run as virtual or cloud-native components on common hardware, misconfigurations, orchestration errors or vulnerabilities in shared subsystems can lead to unintended interactions between slices. This increases the importance of robust management-layer controls and secure orchestration mechanisms capable of enforcing strict separation throughout the slice lifecycle [20].

As a result, the 5G system introduces new surfaces of exposure, ranging from shared virtualised infrastructure to service-based interfaces between network functions. While

these considerations do not yet describe concrete attack vectors, they highlight structural characteristics that must be examined when assessing the security of network slicing. The following Literature Review builds on these foundational principles, analysing how current research addresses isolation challenges and security risks across the 5G architecture.

2.2 Literature Review

This section presents a critical review of the existing literature on security challenges in 5G network slicing. The review focuses on theoretical models, taxonomies, known vulnerabilities, and proposed mitigation strategies, including emerging AI-based solutions. Particular attention is given to the gap between conceptual research and practical implementations, which remains one of the most pressing limitations in current studies. The works analysed were selected for their relevance to slice isolation, orchestration security, and end-to-end threat mitigation. The goal of this review is to identify the most significant contributions in the field while highlighting research gaps that inform the methodological choices and theoretical proposals developed in this dissertation.

2.2.1 Theoretical Security Models and Taxonomies

A significant body of literature has been dedicated to establishing theoretical frameworks and taxonomies to understand and classify the security challenges inherent to 5G network slicing.

Khan et al. [23] provide a comprehensive taxonomy that encompasses design principles, orchestration layers, and security requirements for slicing in next-generation networks. Their analysis emphasizes the critical need for elasticity, scalability, and secure resource isolation, particularly in the context of IoT-driven intelligent applications.

Similarly, Madi et al. [26] introduce a three-dimensional threat taxonomy focused on the NFV infrastructure within 5G environments. Their model categorizes threats based on virtualisation vulnerabilities, insecure communication channels, and operational misconfigurations, offering a structured perspective on multi-domain and multi-tenant security issues. These taxonomies serve as a foundation for understanding complex threat surfaces in dynamic and heterogeneous 5G ecosystems.

Rafique et al. [34] contribute to this discourse by proposing a taxonomy for beyond-5G (B5G) slicing architectures, integrating AI/ML-based orchestration, SDN/NFV capabilities, and edge computing. Their approach aims to optimize slice deployment for smart city use cases, but also identifies persistent challenges such as inter-slice isolation and cross-domain orchestration.

While these models provide valuable conceptual tools, a recurring limitation is the absence of consistent validation through real-world deployments or open-source implementations. Moreover, existing taxonomies often lack granularity when distinguishing between the different architectural layers of 5G slicing (e.g., orchestration vs. virtualisation vs. network layers), a gap that this dissertation addresses through a more fine-grained classification introduced in Chapter 4.

2.2.2 Known Vulnerabilities and Attack Vectors

Several studies explore specific vulnerabilities and threat vectors in 5G network slicing, with a shared emphasis on the risks associated with resource sharing, virtualisation, and dynamic orchestration.

Olimid et al. [30] provide a focused analysis of security threats across the entire slice lifecycle, highlighting both intra-slice and inter-slice vulnerabilities. Their work identifies core risks such as data leakage between slices, misconfigured orchestration policies, and weak authentication mechanisms. Recommended countermeasures include robust slice isolation and the use of advanced cryptographic protocols.

Barakabitze et al. [7] echo similar concerns in their review of SDN and NFV-based slicing architectures. They identify slice isolation, orchestration scalability, and secure multi-domain management as open challenges. Notably, they stress the need for security to be embedded by design, particularly in service function chaining and edge-based deployments.

Knieps [24] extends the discussion by incorporating regulatory and economic perspectives, arguing that cybersecurity in network slicing must also address compliance with directives such as NIS2 and emerging standards for cross-border data flows. This highlights the multifaceted nature of slice security, which encompasses not only technical controls but also governance, policy, and trust frameworks.

Beyond purely technical risks, structural and economic transformations driven by 5G and network slicing also introduce new security and governance considerations. The authors in [9] argue that the transition towards software-defined, slice-based architectures may profoundly reshape both the vertical and horizontal structure of the mobile ecosystem, reducing the number of independent (R)AN operators and increasing reliance on shared or wholesale connectivity models. The progressive digitalisation of the broader economy amplifies competition among heterogeneous service providers for end-user relationships, thereby increasing the likelihood that mobile operators become commodity-level wholesale suppliers operating within multi-tenant environments. These market-driven reconfigurations have direct implications for cybersecurity, as they heighten the complexity of accountability, cross-domain trust, and regulatory oversight — particularly when powerful application and content providers gain greater leverage over connectivity layers.

Taken together, these studies reveal a diverse array of threats that span all architectural layers of network slicing, from physical infrastructure to orchestration logic. However, a common shortcoming is the limited experimental validation of these threats in realistic environments, an issue further examined in Chapter 3.

2.2.3 Mitigation Strategies and AI-based Approaches

Recent literature has proposed several mitigation strategies aimed at enhancing the security and resilience of 5G network slicing. These include both architectural solutions and intelligent detection frameworks.

Thantharate et al. [37] introduce Secure5G, a deep learning-based approach to proactively identify and block malicious connections before they affect network slices. Their framework targets layered security improvements across (R)AN, Multi-access Edge Computing (MEC), and core components, addressing Distributed Denial of Service (DDoS) and other volumetric attacks.

Matencio et al. [11] propose a scalable cognitive framework for autonomous slice management in IoT-rich 5G environments. Their solution emphasizes low-latency and high-throughput service delivery for URLLC and eMBB traffic types, supported by an enhanced Open vSwitch implementation.

A related contribution presented in [27] introduces a Deep Reinforcement Learning

(DRL) agent designed to optimise dynamic resource allocation for 5G network slicing across heterogeneous service scenarios, specifically eMBB–URLLC and eMBB–mMTC. The proposed model evaluates multiple decoding schemes — OMA, NOMA, and RSMA — and autonomously selects the most efficient option based on traffic demand, power gains, device density, and available spectrum resources. Experimental results demonstrate that the agent consistently maximises either the aggregate sum rate or the number of successfully decoded devices, achieving efficiencies between 84% and 100% across varying conditions. Although the study primarily targets performance optimisation rather than explicit security objectives, its findings illustrate how intelligent and context-aware orchestration can indirectly reinforce slice robustness by mitigating resource contention, preventing QoS degradation, and supporting more predictable inter-slice isolation.

These AI-driven approaches offer promising directions for adaptive and automated slice protection. Nevertheless, most remain at the proof-of-concept stage, with limited applicability to current open-source slicing platforms, which lack native support for such advanced orchestration and security mechanisms.

2.2.4 Practical Implementations and Gaps

A smaller body of work examines the implementation of slicing in practical or experimental environments. Al-Falahy and Alani [12] discuss the architectural enablers of 5G, such as cloud-based radio access networks (C-RAN) and NFV, framing them as prerequisites for advanced slicing capabilities. However, their analysis is predominantly theoretical, with limited insight into deployment constraints.

More implementation-oriented research is presented by Nerini et al. [29], who investigate network slicing in Wi-Fi systems as a complementary access technology for 5G. Their work demonstrates slice differentiation using SSID-based resource allocation and evaluates performance metrics through ns-3 simulations. The findings show promising improvements in latency, spectral efficiency, and traffic isolation.

A more security-oriented implementation perspective is offered by recent work proposing a blockchain-based framework for authentication and authorisation in multi-operator slicing environments [41]. The authors introduce a distributed certificate management system that leverages elliptic-curve cryptography and Hyperledger Fabric chaincode to

automate certificate issuance, validation, and revocation across heterogeneous domains. In parallel, they design an authorisation mechanism for shared Network Functions (NFs), aiming to prevent misuse of services, deceptive denial-of-service behaviours, and cross-slice data leakage. Experimental evaluation shows that the framework mitigates single points of failure inherent to traditional certificate authorities, while formal verification using ROR logic and the Scyther tool confirms the security guarantees of the proposed protocols. This line of work highlights the growing emphasis on robust, distributed trust mechanisms as slicing deployments mature.

Despite these contributions, the broader literature remains sparse in terms of validated, large-scale slicing implementations using real-world testbeds. This gap becomes particularly relevant when evaluating the feasibility of executing security-focused experiments on platforms such as Free5GC and OSM, as explored in Chapter 3.

2.2.5 Summary of Research Gaps

In summary, the existing literature provides valuable theoretical foundations, taxonomies, and mitigation strategies for addressing the security challenges of 5G network slicing. At the same time, the review reveals a set of persistent limitations that continue to affect the maturity of the field and the practical applicability of existing proposals. In particular, three recurring research gaps can be identified: the misalignment between theoretical models and practical implementation constraints, the limited empirical validation of vulnerabilities and mitigation strategies, and the still immature integration of AI/Marchine Learning (ML)-based orchestration into existing platforms. These gaps are summarised in Table 2.2.

Taken together, these gaps justify the analytical and theoretical focus adopted in this dissertation.

2.3 Critical Analysis of Available Tools and Platforms

The assessment of available tools and platforms for 5G network slicing is crucial to understand their suitability for research purposes. Despite offering functionalities for orchestration, emulation, and slice management, these tools vary greatly in completeness

Table 2.2: Summary of key research gaps identified in the literature

Gap Category	**Description in the Literature**	**Implication for this Dissertation**
Theory–Practice Misalignment	The literature proposes numerous theoretical models and taxonomies, but gives limited attention to the practical constraints and immaturity of open-source slicing platforms.	Supports the critical assessment of implementation constraints and explains the reformulation of the dissertation towards a theoretical framework.
Limited Empirical Validation	Many studies rely on simulations or conceptual analyses, with relatively few validated experiments in realistic multi-slice environments.	Justifies the use of structured attack scenario analysis and theoretical modelling instead of full empirical validation.
Immature AI/ML Integration	AI/ML-based security and orchestration solutions are increasingly discussed, but their practical integration into real slicing platforms remains limited, non-standardised, and insufficiently validated.	Motivates the inclusion of adaptive monitoring and automated response as conceptual components of the proposed security framework.

and reliability. This section provides a critical analysis of the main open-source solutions, highlighting their capabilities, limitations, and relevance for experimental studies.

2.3.1 Overview of Open-Source Tools for 5G Slicing

A variety of open-source tools have been developed to support experimentation with 5G architectures, including components for network slicing, orchestration, and simulation. Among the most widely adopted in academic and research contexts are Open Source MANO, Free5GC, and UERANSIM. These tools aim to replicate key elements of 5G infrastructure and functionality, albeit with varying degrees of completeness, stability, and compatibility.

OSM is an ETSI-hosted project intended to provide orchestration and lifecycle management of Virtualized Network Functionss (VNFs) and Network Services (NSs). In theory, OSM offers support for network slice definition and instantiation via Network Service Descriptors (NSDs) and Virtualized Network Function Descriptors (VNFD). However, as of

version 9, OSM mandates the use of SOL006[1]-compliant packages, which rely on YANG[2] data models to describe network services in a standardized and machine-readable format. This transition from the earlier SOL001[3] descriptors increases modelling precision but also introduces compatibility and implementation challenges. Manual conversion attempts often fail due to incomplete documentation and complex schema structures. As a result, using OSM for slice orchestration in security testing scenarios requires significant development effort and deep understanding of SOL006, which was considered beyond the feasible scope of this work.

Free5GC is an open-source implementation of the 5G Core (5GC) network. It includes components such as AMF, SMF, UPF and supports slice identifiers Single Network Slice Selection Assistance Information (S-NSSAI). Despite successful installation on Ubuntu 20.04 and partial testing in combination with UERANSIM, the platform exhibited instability during repeated executions. Issues included unexpected component failures (e.g., AMF or UPF crashes) and inconsistent behaviour even with clean installations. Although Free5GC implements logical slice identifiers, it does not enforce physical or functional isolation between slices, which undermines its applicability for security testing focused on inter-slice attacks or policy enforcement.

UERANSIM serves as a 5G User Equipment (UE) and Next Generation NodeB (gNB) simulator, commonly used alongside Free5GC. In isolated scenarios, UERANSIM functions correctly and allows registration attempts and basic traffic flows. However, integration with Free5GC is fragile and subject to version incompatibilities. These conflicts often lead to failures in authentication, IP assignment, or session establishment, making it difficult to maintain a stable test environment.

Other tools were also considered during the exploratory phase. **Open Air interface (OAI)** offers a complete 5G (R)AN and Core implementation but was excluded due to its steep learning curve and limited documentation. **Open5GS**, a modular alternative to

[1]SOL006 is an ETSI specification that defines the information model and data formats for network function descriptors (VNFDs) and network service descriptors (NSDs), enabling standardized automation and interoperability in MANO frameworks.

[2]YANG is a data modelling language defined by the Internet Engineering Task Force (IETF) for describing the configuration and operational data of network elements in a structured and machine-readable form.

[3]SOL001 is an earlier ETSI specification defining the packaging and descriptor formats for network functions and services in MANO systems, preceding the data-model-driven SOL006 approach.

Free5GC, was not tested directly as it did not present clear advantages and would likely face similar architectural limitations. Orchestration tools such as **Tacker** (OpenStack) were also excluded due to their complexity and limited relevance to slice-specific testing. Simulation environments like **NS-3**, **Mininet**, and **NetSim** were reviewed but ultimately considered unsuitable for this work, either due to lack of slicing support, limited realism, or commercial access restrictions.

Commercial solutions such as **Nokia NetAct**[4], **Ericsson Orchestrator**[5], **Huawei CloudCore**[6], or **VMware Telco Cloud Automation**[7] [39] [38] also provide mature 5G core and orchestration capabilities, often with integrated slice lifecycle management and policy enforcement features. These commercial platforms are designed primarily for carrier-grade deployments, providing robust service orchestration, network automation, and policy-driven slice management. They integrate tightly with vendor-specific ecosystems and often include advanced monitoring, analytics, and SLA assurance modules. However, their proprietary nature, high licensing costs, and restricted research access make them unsuitable for open academic experimentation. As such, the analysis in this work focuses exclusively on open-source and publicly accessible platforms.

This overview confirms that, while the open-source ecosystem offers several promising platforms for 5G research, none provide a complete, stable, and security-focused environment for network slicing experimentation. These findings directly inform the analysis of capabilities and limitations presented in the following section.

[4]Nokia NetAct is Nokia's network management and orchestration suite for mobile and fixed networks, providing automation, configuration, and assurance functions across Fourth Generation (4G) and 5G infrastructures:
`https://customer.nokia.com/support/s/product2/netact/01t41000004gAuNAAU`

[5]Ericsson Orchestrator is part of Ericsson's Dynamic Orchestration portfolio, enabling network slice lifecycle management, service assurance, and policy-based automation:
`https://www.ericsson.com/en/portfolio/cloud-software-and-services/network-management-and-automation/ericsson-orchestrator`

[6]Huawei CloudCore is a 5G core network solution offering full-service orchestration, network slicing, and cloud-native deployment capabilities for carrier networks:
`https://carrier.huawei.com/en/solutionsv2/equipment-cloudification/CloudCore`

[7]VMware Telco Cloud Automation provides network service orchestration and multi-cloud management for NFV- and 5G-based infrastructures, supporting automated slice deployment and assurance:
`https://www.vmware.com/products/cloud-infrastructure/telco-cloud-platform`

2.3.2 Tool Capabilities and Limitations

The tools explored in this study offer varying degrees of alignment with the theoretical requirements of 5G network slicing. However, none fully meet the functional, architectural, and security criteria necessary for realistic security testing or experimentation.

OSM demonstrates high-level orchestration capabilities through its support for VNF and NS descriptor models, lifecycle management, and integration with NFV infrastructures. Nevertheless, its reliance on SOL006-compliant packages introduces a steep barrier to entry, particularly in the absence of publicly available VNFs in the required format. This limitation severely constrains its usability for rapid prototyping and testing in academic contexts. Additionally, the lack of intuitive tooling or conversion utilities hampers onboarding and adaptation to existing projects.

Free5GC offers a modular and transparent implementation of the 5G Core, which is valuable for understanding internal operations. However, its slice support remains limited to logical S-NSSAI tagging, with all slices sharing the same UPF and other infrastructure components. This undermines efforts to model isolation failures or security boundaries between slices. Furthermore, its unstable runtime behaviour — including frequent component crashes and unpredictable behaviour across installations — limits its reliability as a testing platform.

UERANSIM is functionally adequate for simulating UEs and (R)AN components. It supports registration, traffic generation, and handover simulation. However, its utility is restricted by tight version dependencies with Free5GC and limited configuration flexibility for simulating heterogeneous slicing conditions. These factors reduce its effectiveness for security experiments that require consistent behaviour across repeated runs.

Security Considerations and Observations

Beyond functional and architectural constraints, all evaluated tools exhibit notable security limitations. Slice isolation is only implemented at the control level (via S-NSSAI), with no enforcement of traffic segregation or policy differentiation at the data plane. There is minimal support for security instrumentation such as traffic monitoring, access control, or anomaly detection. Most tools also lack audit mechanisms or granular logging capabil-

ities, making it difficult to trace security events or validate mitigation mechanisms. These shortcomings highlight a critical gap between the security assumptions in theoretical models and the capabilities of real-world open-source platforms. A summary of these findings is provided in Table 3.1.

2.3.3 Summary and Implications for Research

The critical analysis of available open-source tools for 5G network slicing reveals a significant disconnect between theoretical models and the practical realities of current platforms. While tools such as OSM, Free5GC, and UERANSIM provide valuable building blocks for experimentation, they fall short in key areas related to orchestration maturity, slice-level isolation, and security instrumentation. These limitations are not merely technical inconveniences; they directly impact the feasibility of executing rigorous, controlled experiments to test security assumptions or validate theoretical attack models.

The inability to enforce true resource separation between slices, monitor traffic effectively, or simulate attack scenarios in a reproducible manner poses serious obstacles to empirical research in this domain. Moreover, the instability and lack of standardization across tool versions hinder the creation of consistent and verifiable testbeds.

These findings have shaped the methodological direction of this dissertation. Rather than pursuing a flawed or incomplete experimental setup, the research adopts a theoretical and analytical approach grounded in the limitations observed. The issues encountered with open-source platforms are treated not as peripheral failures, but as critical data points that reflect the current state of technological readiness in 5G slicing environments. This perspective informs the development of a fine-grained vulnerability taxonomy and a conceptual framework for secure slice isolation, as detailed in the chapters that follow.

Chapter 3

Experimental Research Methodology

This chapter outlines the initial experimental methodology conceived to assess security vulnerabilities and isolation mechanisms in 5G network slicing environments. The research began with a practical approach, aiming to simulate multi-slice scenarios using open-source tools in order to test inter-slice attacks and validate mitigation strategies. However, as the implementation progressed, critical technical limitations emerged, which compromised the feasibility and reproducibility of the experimental setup. Rather than disregarding these obstacles, they were systematically documented and analysed as relevant research findings. This chapter thus details the evolution of the methodological strategy, the practical challenges encountered, and the rationale for transitioning to a theoretical and analytical framework, grounded in the observed limitations of current open-source 5G platforms.

3.1 Initial Experimental Strategy

The initial phase of this dissertation was designed with a strong experimental focus, aiming to investigate the security of 5G network slicing through the deployment of realistic test environments. The primary goal was to explore the extent to which slice isolation could be ensured in practice, particularly at the network layer, and to evaluate the impact of potential vulnerabilities on performance and confidentiality.

To this end, the strategy involved the simulation of multi-slice 5G scenarios using open-source tools capable of instantiating and managing virtualised network components. The plan included the deliberate emulation of inter-slice attack vectors—such as traffic

leakage, shared resource contention, and unauthorised access between slices—in order to assess whether logical separation mechanisms would hold under adversarial conditions. A complementary objective was to experiment with mitigation mechanisms, including traffic filtering and resource isolation policies, applied dynamically during test execution.

The first tool selected was OSM, chosen for its capabilities in orchestrating VNF and NS. The expectation was to use OSM to create isolated slices through SOL-compliant descriptors, instantiating network functions with different security configurations and routing policies. This approach would enable a modular and scalable testing environment aligned with ETSI and 3GPP standards.

However, due to technical limitations encountered with OSM, especially the requirement for SOL006 descriptors and the lack of available VNFs in this format—the strategy was revised. As an alternative, the open-source 5G core implementation Free5GC was selected to serve as the central element of a more manual test environment. Its modular architecture, support for the S-NSSAI identifier, and accessible documentation made it a suitable candidate for low-level slice configuration. In combination, UERANSIM was incorporated as a simulator for UE and gNB, enabling registration, traffic flows, and basic radio access emulation.

In this revised setup, slices were to be configured within Free5GC and tested for logical separation, with UERANSIM generating traffic across different S-NSSAIs. The goal remained the same: to evaluate whether current open-source tools could support security testing of inter-slice isolation and provide mechanisms for detecting or mitigating violations.

This experimental strategy represented a structured and technically grounded attempt to bridge the gap between theoretical security models and their practical evaluation within realistic 5G network conditions.

3.2 Test Environment and Configurations

The experimental setup for this dissertation relied on two distinct virtualised environments, each tailored to the specific tools under evaluation. The first environment was created to host the OSM orchestration platform, while the second was dedicated to testing

Free5GC and UERANSIM in a standalone 5G core simulation scenario.

The OSM instance was deployed on a Dell PowerEdge R620 server running Ubuntu 22.04.5 Long-Term Support (LTS). The environment featured 16 GB of Random Access Memory (RAM), 6 Virtual Central Processing Units (vCPUs), and 120 GB of disk storage. OSM version osm-16.0-sixteen was installed using the official installation guide[1] provided by ETSI. Minor modifications were applied to the installation script to address a recurring error related to the Airflow module not being deployed correctly within the required time-frame. Specifically, the script was adapted to install Airflow manually using Helm after the Kubernetes components were initialized. This allowed the installation process to complete successfully, although further progress was hindered by incompatibilities with descriptor formats, as later discussed.

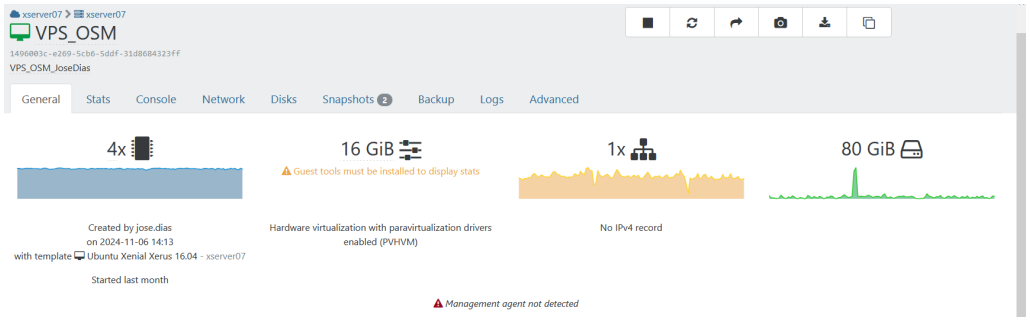

Figure 3.1: OSM Setup Virtual Machine (VM)

The Free5GC and UERANSIM environment was hosted on a local machine using VirtualBox. This VM was configured with 4 vCPUs, 8 GB of RAM, and 40 GB of storage, running Ubuntu 20.04 LTS (64-bit) with bridged networking and internet access. The Free5GC core used in this setup was version v3.3.0, cloned from the official GitHub repository. This version follows a modular architecture comprising independent NFs such as AMF, SMF, NRF, and UPF, and relies on MongoDB as the backend database. UERANSIM version v3.2.6 was selected to ensure compatibility with Free5GC and was configured to simulate both UE and gNB behaviour, including registration attempts and Protocol Data Unit (PDU) session establishment.

The configuration of the Free5GC stack followed the official HackMD handbook[2] . A full registration test scenario, named TestRegistration, was attempted using the ./test.sh

[1] https://osm.etsi.org/docs/user-guide/latest/03-installing-osm.html
[2] https://hackmd.io/@free5GC/free5gc_handbook

script included in the Free5GC repository. This scenario simulates end-to-end communication between UERANSIM and Free5GC, involving the setup of a gNB, the exchange of registration messages, and the activation of PDU sessions via AMF, SMF, AUSF, and UDM.

Despite partial component registration and network function bootstrapping, the test environment never achieved a fully stable state suitable for reproducible experimentation.

Repeated attempts to run the test revealed persistent issues:

- MongoDB was often not initialized or responsive (connection refused on `127.0.0.1:27017`);
- The NRF failed to bind to the configured port (`127.0.0.1:8000` already in use);
- Individual components crashed or failed to register properly, even in clean installations.

Troubleshooting efforts included:

- Live inspection of log files (`~/free5gc/log/<timestamp>/free5gc.log`);
- Use of `"tail -f"`, `"grep"`, and `"ss - ltnp"` to trace service status and port conflicts;
- Monitoring of MongoDB responsiveness and process states using ps and mongo shell commands.

These efforts confirmed that, despite following the official setup procedures and using compatible software versions, the environment remained unstable and unsuitable for controlled testing of slice isolation and security mechanisms. No usable test results could be generated, as registration procedures frequently failed due to component crashes or unresolved dependencies.

Snapshots were taken at key stages of installation and configuration to facilitate rollback and recovery. Despite these precautions, consistent functionality could not be achieved. In the case of OSM, the inability to create and instantiate slices using SOL006-compliant packages prevented even the initiation of security-focused experiments. These challenges, while initially viewed as setbacks, ultimately became important data points in shaping the revised research methodology, as described in the next sections.

3.3 Technical Challenges and Limitations Encountered

The experimental phase encountered a series of recurring technical challenges that severely limited the viability of the intended security testing. These challenges, although initially perceived as implementation barriers ultimately served as valuable indicators of the current maturity and readiness of open-source platforms for research in 5G network slicing.

One of the most significant obstacles emerged during the attempt to use OSM for orchestrating network slices. As of version 9, OSM requires all NSDs and VNFDs to follow the SOL006 format, which is based on YANG models and fundamentally different from the more widely used SOL001 format. This shift rendered most publicly available VNF packages, including those for Free5GC, incompatible by default. Attempts to convert legacy packages to the new format proved unsuccessful due to the complexity of the YANG models and the lack of comprehensive documentation or tooling. Without pre-built, SOL006-compliant VNF packages or accessible templates, the creation of even basic network slices was not achievable within a reasonable timeframe. As a result, the use of OSM was deemed unfeasible for this dissertation.

In the subsequent strategy, the focus shifted to a manual setup using Free5GC and UERANSIM. While installation and partial configuration were successful, the environment proved to be unstable and unreliable for repeated execution of security scenarios. Several core limitations were observed:

- Intermittent component crashes, including the AMF and UPF, occurred even after clean installations;
- Version incompatibilities between Free5GC and UERANSIM led to failed authentication, IP assignment issues, and broken communication workflows;
- The MongoDB backend—a critical dependency—frequently failed to initialize or respond, preventing proper registration of network functions;
- The NRF encountered binding conflicts due to port collisions (e.g., `127.0.0.1:8000` already in use), halting component registration;

- Most importantly, while Free5GC supports the S-NSSAI identifier for slice tagging, this separation is purely logical. All slices share the same UPF and transport infrastructure, meaning no actual traffic isolation or resource separation is enforced. As such, testing for inter-slice attack vectors or slice-specific security policies was technically impossible in this environment.

These limitations directly undermined the core experimental goals of this dissertation, which included testing isolation failures, simulating cross-slice attacks, and evaluating mitigation mechanisms. Without the ability to isolate traffic or simulate adversarial conditions in a controlled and repeatable way, the environment failed to support any meaningful security experiments.

To better visualize and consolidate the nature of these challenges, Table 3.1 presents a comparative overview of the tools used, highlighting their key characteristics, limitations, and relevance to the research objectives.

Table 3.1: Summary of Experimental Findings and Limitations

Tool	**Test Outcome**	**Main Limitations**	**Relevance to Research**
OSM (v16)	Not functional	Requires SOL006 packages; lack of VNF support	Unusable for slice orchestration
Free5GC (v3.3.0)	Partially functional	Instability; no real slice isolation	Limited for attack simulation
UERANSIM (v3.2.6)	Partially functional	Version conflicts; unstable with Free5GC	Insufficient alone for testing

The nature of these challenges also reflects broader concerns about the maturity of open-source tools in the 5G space. While platforms like Free5GC and OSM provide valuable insights into 5G architecture, their current implementations lack the robustness, flexibility, and feature completeness required for advanced experimentation. Security is often treated as an afterthought in these platforms, with minimal logging, no built-in monitoring, and no native support for enforcing security policies or capturing anomalies at the slice level.

Ultimately, these limitations were not viewed solely as technical setbacks but as empirical evidence of the gap between theoretical models and practical implementations. Rather

than proceeding with flawed or partial experiments, the challenges documented in this section justified a shift in the methodological approach—moving from hands-on testing to a conceptual and analytical investigation, which is discussed in the following section.

3.4 Reframing the Research Approach

The experimental challenges encountered during the implementation phase—ranging from VNF descriptor incompatibilities in OSM to persistent instability and lack of isolation in Free5GC—revealed not merely technical setbacks, but critical insights into the current state of open-source 5G platforms. Rather than dismissing these obstacles as peripheral or accidental, they were reinterpreted as valid scientific data points. These difficulties reflect systemic limitations that directly impact the feasibility of reproducing or validating theoretical models in practical environments.

The methodological evolution of this work is summarised in Figure 3.2, which outlines the transition from the initial experimental objectives to the final analytical framework.

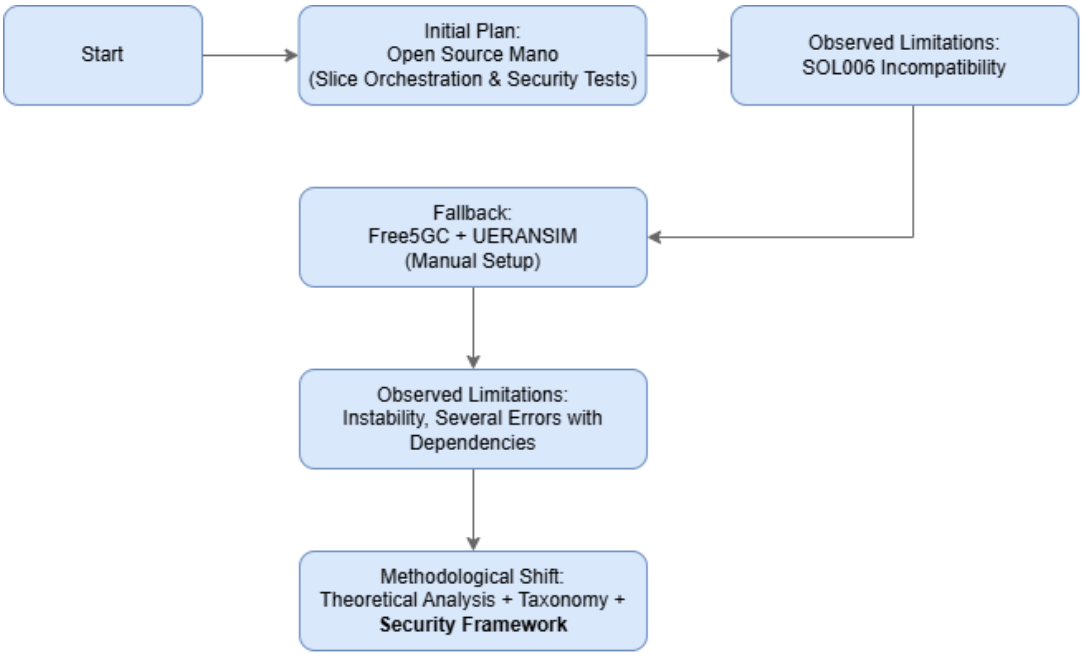

Figure 3.2: Evolution of the research approach

These observations align closely with the research gaps identified in the literature review (Chapter 2). While many academic works propose sophisticated security architectures and isolation mechanisms for Sixth Generation (6G) slicing, few address the readiness of

available tools to support such mechanisms. The inability to instantiate multiple isolated slices, enforce distinct security policies, or reliably simulate attack vectors exposes a disconnect between theoretical expectations and the operational reality of current platforms. This reinforces the relevance of a critical, theory-grounded approach.

In response to these constraints, the research methodology was reframed to emphasize theoretical and analytical contributions. Rather than persisting with limited or unreliable experiments, the study adopted a systematic examination of the assumptions, requirements, and vulnerabilities associated with slice isolation. The new methodology is composed of three main pillars:

- A document-based analysis of real-world limitations, grounded in empirical observations from the attempted implementations;
- The development of a fine-grained taxonomy of vulnerabilities that reflects both theoretical attack surfaces and practical feasibility constraints;
- The proposal of a conceptual framework for secure slice isolation, designed to bridge the gap between abstract models and implementable security guidelines.

This reformulated approach ensures the scientific relevance of the dissertation by producing generalizable insights, even in the absence of fully functional experimental infrastructure. Moreover, it enables critical reflection on the maturity of current 5G tools, contributing not only to the academic discourse but also to future design requirements for slicing-capable, security-aware network platforms.

3.5 Summary

This chapter documented the evolution of the research methodology, starting from an initially planned experimental strategy and transitioning towards a theory-driven analytical approach. The original objective was to simulate 5G slice environments using open-source platforms—primarily OSM and Free5GC in order to test inter-slice isolation and simulate security attacks under controlled conditions. However, significant technical challenges were encountered, including software incompatibilities, lack of mature slice orchestration support, and absence of real traffic isolation.

Rather than undermining the research effort, these challenges provided valuable insight into the current limitations of widely used 5G testbed tools. The resulting data informed a shift in methodological focus, allowing the study to frame these obstacles as evidence of a broader gap between theoretical security frameworks and real-world implementation readiness.

As a result, the work pivoted toward a reformulated methodology based on literature synthesis, vulnerability modelling, and the development of a conceptual framework for secure slice isolation. This approach maintains scientific rigor while addressing the practical constraints inherent to contemporary open-source 5G platforms.

The next chapter builds upon this foundation by presenting a detailed vulnerability taxonomy, structured according to architectural layers and slicing components. It also explores key attack vectors and outlines the design of a mitigation framework tailored to multi-tenant 5G slicing environments.

Chapter 4

Detailed Vulnerability Analysis

As the previous chapters have demonstrated, current open-source platforms for 5G slicing lack the technical maturity and isolation capabilities necessary to support robust empirical testing. In light of these limitations, this chapter shifts the focus towards a structured, theoretical exploration of key vulnerabilities affecting network slice isolation.

Rather than relying on incomplete or unstable experimental environments, the analysis presented here draws upon architectural models, documented security threats [14], and domain-specific risk frameworks to examine how slicing-specific vulnerabilities could emerge and propagate. The goal is to identify potential attack surfaces, evaluate their impact on slice isolation, and determine the underlying conditions that enable such weaknesses.

To this end, the chapter is organized around a multi-layered classification of vulnerabilities, following the taxonomy introduced earlier. For each category, relevant threat vectors are modeled and assessed in terms of their impact on isolation, trust boundaries, and security policy enforcement. Where possible, reference is made to real-world incidents or proof-of-concept exploits described in the literature.

By combining threat modelling with a conceptual understanding of 5G architecture, this chapter contributes to the definition of a comprehensive threat landscape for network slicing. The results form the analytical foundation for the secure slicing framework proposed in the following chapter. 5

4.1 Taxonomy of Vulnerabilities in Network Slicing

Given the inherent architectural complexity and multi-layered structure of 5G networks, security vulnerabilities can arise from multiple points within the slicing stack. To systematically capture these threats, this section presents a taxonomy of vulnerabilities structured according to the functional layers of the 5G slicing architecture. This classification is grounded in a detailed literature review and was previously introduced in peer-reviewed research, now adapted and expanded to serve as a core analytical framework for the present dissertation.

To ensure that the taxonomy was grounded in systematic and reproducible evidence, a structured literature review was conducted prior to its development. The search process covered major scientific databases, including Institute of Electrical and Electronics Engineers (IEEE) Xplore, Association for Computing Machinery (ACM) Digital Library, Scopus, SpringerLink, and Multidisciplinary Digital Publishing Institute (MPDI). Keyword queries such as "5G network slicing security", "slice isolation", "SDN NFV vulnerabilities", "5G orchestration security", "multi-tenant 5G threats", and "MANO security vulnerabilities" were applied to titles and abstracts. This process returned a substantial corpus of publications, from which only works directly addressing slicing architectures, SDN/NFV-based management, or multi-tenant orchestration were retained. After screening titles and abstracts for relevance, a subset of studies was examined in detail, and the taxonomy was derived from the recurring vulnerability patterns identified across these sources. The resulting classification was further complemented with information from public vulnerability databases (e.g., Common vulnerabilities and Exposures (CVE)) and documented security incidents, ensuring that it remains aligned with both peer-reviewed research and realistic threat models.

The taxonomy is organized into four architectural layers:

- Orchestration and Management Layer;
- Virtualisation Layer;
- Network Layer;
- Interface and Communication Layer.

Each layer is further subdivided into specific vulnerability categories that correspond to distinct attack surfaces or weak points in the system. This layered approach reflects the operational lifecycle of network slices—from their orchestration and deployment, through virtualisation and execution, to real-time communication and inter-slice interactions. By mapping threats to these domains, the taxonomy provides both a descriptive and analytical tool for understanding how vulnerabilities can propagate through the slicing infrastructure and compromise security guarantees such as isolation, integrity, and confidentiality.

The classification was derived from a structured analysis of current academic and technical literature on 5G security, with particular attention to attack vectors linked to SDN, NFV, and multi-tenant orchestration platforms such as Open Source MANO. Public vulnerability databases (e.g., CVE) and incident reports were also used to ground the taxonomy in realistic threat models.

Figure 4.1 presents a visual overview of the taxonomy, highlighting the hierarchical structure of layers and subcategories. Table 4.1 complements this view by describing concrete examples of threats associated with each subcategory.

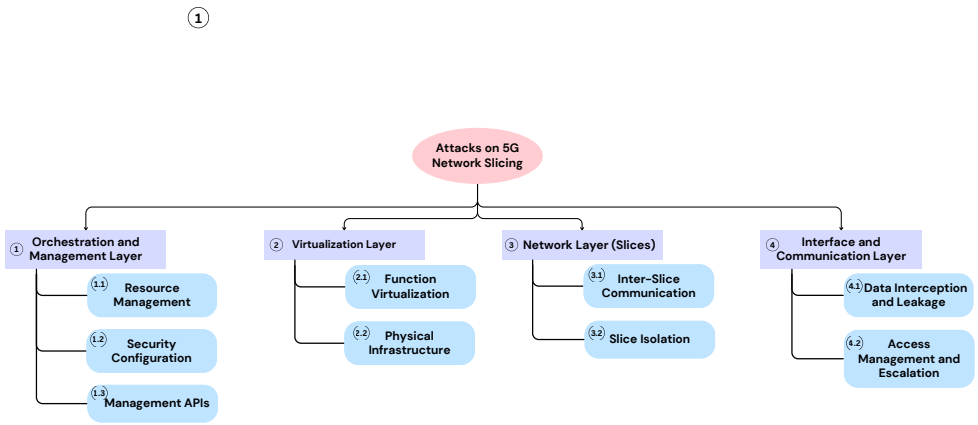

Figure 4.1: Taxonomy of attack vectors across 5G network slicing architecture layers

Table 4.1 complements the proposed classification by detailing specific attack vectors associated with each architectural layer and subcategory. Each entry in the table reflects the numbering system of the classification, ensuring consistency between the hierarchical classification and the identified threat vectors. This structured overview facilitates a

clearer understanding of how different attack surfaces relate to the respective network slicing components and highlights critical areas requiring targeted security measures.

Table 4.1: Security threats across 5G network slicing architecture layers

Layer	**Subcategory**	**Description of Threat**
1—Orchestration and Management Layer	**1.1—Resource Management**	Attacks aim to disrupt resource allocation across slices, often through resource exhaustion (e.g., flooding orchestrators with fake requests), leading to service degradation or DoS. Attacks on orchestrators or managers can result in unauthorised reallocation or slice disruption.
	1.2—Security Configuration	Exploiting vulnerabilities in orchestrators (e.g., OSM) can lead to unauthorised access and misconfigured slices. Attackers may weaken security policies such as authentication and encryption to escalate privileges or extract data.
	1.3—Management APIs	Poorly secured APIs enable attackers to access slice management functions. Weak authentication or excessive permissions can lead to unauthorised modifications, data leakage, or service disruption. Real incidents have shown how exposed APIs in orchestration platforms pose significant risks.
2—virtualisation Layer	**2.1—Function virtualisation**	Attacks on the hypervisor or NFVs can allow privilege escalation, manipulation of services, or code injection. This may result in instability or outages across multiple slices sharing infrastructure.
	2.2—Physical Infrastructure	Hardware-level attacks (e.g., tampering or DoS on components) can disrupt all slices dependent on the affected infrastructure due to the shared nature of physical resources.

Layer	Subcategory	Description of Threat
3—Network Layer	**3.1—Inter-Slice Communication**	Poor isolation may lead to unintended data exchange or unauthorised access between slices. Attackers can exploit these flaws to intercept traffic, leak data, or breach isolated services.
	3.2—Slice Isolation	Resource-sharing mechanisms may be abused to exhaust shared resources, degrading performance, or allowing lateral movement across slices. Weak dependency controls increase this risk.
4—Interface and Communication Layer	**4.1—Interception and Data Leakage**	Techniques such as traffic analysis or credential theft can be used to monitor operations or extract sensitive data. Internal threats and weak security controls contribute to these risks.
	4.2—Access and Escalation Management	Weak authentication or command injection can lead to unauthorised access or privilege escalation. Attackers may move laterally across slices, gaining deeper control over the network.

This taxonomy will serve as the foundation for the threat modelling and scenario analysis carried out in the next section. Each category of vulnerabilities—ranging from API exposure to inter-slice traffic leakage—is not only relevant from a theoretical standpoint, but also critical in shaping effective security mechanisms in future 5G deployments.

4.2 Attack Scenarios and Theoretical Models

The following subsections provide a structured analysis of potential attack scenarios across each subcategory of the proposed taxonomy, detailing attacker objectives, entry vectors, expected impacts, and—where relevant—conceptual models to illustrate the threat dynamics involved.

1.1 - Resource Management

Resource Management is a critical component within the orchestration and management

layer of 5G network slicing. It is responsible for allocating virtualised computing, storage, and networking resources across multiple slices. Weaknesses in this domain can allow attackers to exploit shared infrastructure, leading to denial of service or unintended degradation of service quality across slices.

Example Attack — Slice Flooding via Orchestrator Overload

An attacker gains access to a legitimate tenant account or exploits weak input validation in the orchestrator's API. Using automated scripts, the attacker issues a large volume of slice instantiation and scaling requests within a short period. Although each request complies with the expected format, their volume exceeds normal operational thresholds and causes overload in the orchestration layer. Without adequate rate limiting or tenant isolation, this action results in cascading failures that affect unrelated slices.

Attack Scenario

- **Objective:** Overload the orchestrator to exhaust shared computational and network resources, causing service degradation or denial of service to legitimate slices;
- **Entry Vector:** Abuse of orchestration APIs through legitimate credentials or exploitation of insufficient input validation; high-frequency instantiation requests without proper throttling controls;
- **Impact:** Disruption of slice scheduling, performance degradation across multiple tenants, temporary denial of service on the orchestrator, and potential crash or freeze of resource allocation services.

This aligns with typical Denial of Service (DoS) resilience models in distributed systems and demonstrates how soft resource boundaries in orchestrators are exploitable without breaching authentication mechanisms.

1.2 - Security Configuration

Security configuration flaws within the orchestration layer can lead to systemic weaknesses across all slices. Orchestrators such as OSM often rely on complex Yet Another Markup Language (YAML) descriptors and configuration templates to enforce policies like encryption, authentication, and role-based access control. When these templates are misconfig-

ured—either due to human error or software limitations—slices may be instantiated with reduced or inconsistent security guarantees.

Example Attack — Misconfiguration Exploitation in Slice Deployment

An attacker gains access to the orchestrator's management interface (or API) and submits a modified NSD template that overrides default security settings. The orchestrator, lacking validation or policy enforcement mechanisms, instantiates a slice without mandatory encryption or disables integrity checks for signaling traffic. Alternatively, a misconfigured template in a production environment might accidentally expose internal services via open ports or weak credentials.

Attack Scenario

- **Objective:** Deploy a slice with weakened security policies to enable traffic interception or lateral movement;
- **Entry Vector:** Malicious API interaction or exploitation of template misconfiguration;
- **Impact:** The slice operates without critical protections (e.g., encryption, authentication), allowing unauthorised access, data leakage, or Man-in-the-Middle (MitM) attacks.

This scenario reflects how weak validation and excessive configurability in orchestration platforms can transform benign misconfigurations into security liabilities, reinforcing the critical role of policy enforcement in slice deployment workflows.

1.3 - Management APIs

Management APIs expose critical control functions such as slice creation, scaling, modification, and termination. If these APIs are inadequately secured—through weak authentication, excessive privileges, or insufficient rate limiting—they become high-value targets for attackers. Given that orchestration platforms typically rely on RESTful APIs for automation and remote management, API exposure significantly increases the attack surface of a 5G slicing environment.

Example Attack — unauthorised Slice Modification via API Abuse

An attacker discovers an exposed management API with either no authentication or de-

fault credentials still in use. By crafting Hypertext Transfer Protocol (HTTP) requests that mimic legitimate slice management operations, the attacker modifies an active slice's topology, injects malicious configuration values, or deletes existing VNFs. In more advanced cases, attackers may exploit API misbehaviour (e.g., insecure deserialization or insufficient input validation) to gain remote code execution privileges on the orchestrator itself.

Attack Scenario

- **Objective:** Manipulate active slice configurations or disrupt operations via unauthorised API access;
- **Entry Vector:** Publicly exposed management API with weak or misconfigured authentication;
- **Impact:** unauthorised reconfiguration of slices, potential service outages, injection of malicious components, or privilege escalation within the orchestration layer.

This attack scenario illustrates how exposed or poorly governed APIs can serve as direct entry points for critical control-plane manipulation, highlighting the need for strict authentication, access control, and input validation in orchestration interfaces.

2.1 — Function virtualisation

Function virtualisation refers to the abstraction layer that allows network functions to run as VMs or containers on shared physical infrastructure. Vulnerabilities in the hypervisor, container runtime, or inter-process isolation mechanisms can be exploited to escape the confined execution environment, compromising co-hosted functions and breaking slice isolation. Since multiple VNFs from different slices may share the same host, a breach in this layer can have cascading effects.

Example Attack — Hypervisor Escape Leading to Cross-Slice Compromise

An attacker gains access to a vulnerable VNF through a misconfiguration or exposed service. From within the virtualised instance, the attacker exploits a known vulnerability in the hypervisor (e.g., Quick Emulator (QEMU), Kernel-based Virtual Machine (KVM), or containerd) to escape to the host operating system. Once on the host, the attacker can

enumerate and access other VNFs belonging to different slices, potentially extracting data, disrupting services, or injecting malicious behaviour into isolated functions.

Attack Scenario

- **Objective:** Escape a compromised VNF/container and gain access to adjacent VNFs running in other slices on the same host;
- **Entry Vector:** Vulnerability in the virtualisation layer (e.g., CVE in QEMU, container runtime escape);
- **Impact:** Breach of slice isolation, data exfiltration, potential control over critical VNF, and lateral movement between slices.

This example demonstrates how vulnerabilities in the virtualisation layer undermine the core assumption of slice separation, turning a local compromise into a platform-wide breach with significant security implications for multi-tenant 5G environments.

2.2 — Physical Infrastructure

The physical infrastructure layer includes all hardware components shared across multiple network slices—servers, network interfaces, switches, and storage systems. Since network slicing builds upon virtualised and logically partitioned resources, any successful attack at the physical level compromises the entire shared substrate. Vulnerabilities at this layer often stem from unmonitored physical access, firmware-level exploits, or DoS techniques targeting hardware components.

Example Attack — Targeted Hardware-Induced DoS Affecting All Slices

An attacker with physical or low-level access to the system (e.g., insider threat or compromised baseboard management controller) performs a deliberate resource starvation attack by overloading the Central Processing Unit (CPU) or saturating a shared network interface. Since these components are not slice-aware, all co-hosted slices experience service degradation or complete unavailability.

Attack Scenario

- **Objective:** Degrade the performance or availability of all slices by targeting shared physical components;

- **Entry Vector:** Physical access, firmware exploits, or misconfigured system-level privileges that allow manipulation of hardware resources;
- **Impact:** Service outages across multiple slices, breach of availability guarantees, potential cascading failures due to shared hardware dependencies.

This scenario highlights how the physical layer remains a single point of failure in logically isolated systems, revealing that no amount of virtual segregation can mitigate risks arising from compromised or poorly protected hardware resources.

3.1 — Inter-Slice Communication

The goal of slice isolation in 5G is to ensure that each network slice operates independently, both in terms of functionality and data flow. However, misconfigurations, architectural flaws, or software bugs can lead to unintentional or unauthorised inter-slice communication. This compromises confidentiality, integrity, and trust boundaries between tenants.

Example Attack — unauthorised Data Access via Shared Routing or Misconfigured Interfaces

An attacker controlling a service within one slice exploits routing or firewall misconfigurations to probe and access resources located in a separate slice. For instance, if slices share a common UPF or transport infrastructure without strict traffic segmentation, malicious actors may intercept or redirect packets intended for another tenant.

Attack Scenario

- **Objective:** Bypass slice isolation to gain access to data or services in a different slice;
- **Entry Vector:** Exploitation of shared user plane elements (e.g., UPF), incorrect Virtual Local Area Network (VLAN) tagging, or absence of strict Access Control Lists (ACLs)/firewall rules between slices;
- **Impact:** unauthorised lateral access between slices, data leakage, breach of tenant confidentiality, and regulatory non-compliance.

This example illustrates how logical segmentation alone is insufficient when shared infrastructure lacks strict enforcement mechanisms, turning benign misconfigurations into

critical violations of tenant isolation and data confidentiality.

3.2 — Slice Isolation

Slice isolation refers to the ability to prevent one network slice from interfering with or accessing the resources of another. In practice, many open-source or early 5G implementations provide only logical isolation through identifiers like S-NSSAI, without actual enforcement at the level of compute, memory, or bandwidth. As a result, resource contention, denial-of-service conditions, or cross-slice interference may occur.

Example Attack — Cross-Slice Resource Exhaustion (CPU or Bandwidth Contention)

An attacker within one slice launches a resource-intensive process (e.g., high-volume traffic or compute load) that consumes shared system resources like CPU or network bandwidth. Since slices may rely on the same UPF or run on the same virtualised infrastructure without strict quotas, this leads to performance degradation or denial of service in other slices.

Attack Scenario

- **Objective:** Disrupt the availability and performance of other slices by abusing shared resources;
- **Entry Vector:** Execution of legitimate but intensive operations from within a slice, exploiting the lack of resource limits or enforcement;
- **Impact:** QoS violations, unpredictable latency, service outages for other tenants, and erosion of Service Level Agreement (SLA) guarantees.

By exploiting the lack of strict enforcement on resource separation, this attack demonstrates how shared infrastructure can become a vulnerability surface, allowing malicious tenants to indirectly impact the performance and reliability of other slices.

4.1 — Interception and Data Leakage

This category refers to the risk of unauthorised access to slice-specific data during transmission or processing. In network slicing environments, improper encryption, shared interfaces, or insufficient access controls can allow adversaries—internal or external—to intercept,

eavesdrop, or extract sensitive data flowing between network functions or user equipment. These threats are particularly critical in multi-tenant scenarios where isolation between slices is expected.

Example Attack — Passive Traffic Sniffing Across Slices

An attacker with access to a compromised virtual function (e.g., a misconfigured VNF or hypervisor component) listens to shared network interfaces or logs, capturing traffic from multiple slices. If encryption is weak or inconsistently applied, the attacker may extract confidential user data, authentication credentials, or control-plane information.

Attack Scenario

- **Objective:** Steal confidential information from other slices or network components by exploiting shared infrastructure or poor data protection mechanisms;
- **Entry Vector:** Compromised VNF, privileged access to shared virtual interfaces, or exploitation of misconfigured logging/debug features;
- **Impact:** Breach of data confidentiality, potential General Data Protection Regulation (GDPR) violations, loss of trust in isolation guarantees, and exposure of core network operations.

This scenario highlights how weak encryption practices and shared interfaces can turn internal components into observation points, undermining confidentiality and exposing sensitive data flows despite logical isolation boundaries.

4.2 — Access and Escalation Management

This category refers to vulnerabilities related to weak authentication mechanisms, improper privilege separation, or insufficient access control within and across network slices. In dynamic 5G environments, where VNFs, APIs, and orchestration layers must authenticate and authorize operations, failures in these mechanisms can allow unauthorised access, privilege escalation, or lateral movement across slices.

Example Attack — unauthorised Command Injection into Slice Control Functions

An attacker gains access to a low-privilege service within a slice (e.g., via a misconfigured web service) and exploits weak API authentication to send unauthorised control commands

to the orchestrator or slice controller. This may allow the attacker to escalate privileges, manipulate slice configurations, or disrupt services in other slices.

Attack Scenario

- **Objective:** Escalate privileges or gain unauthorised access to administrative interfaces within or across slices;
- **Entry Vector:** Weakly protected APIs, default credentials, insecure communication channels, or misconfigured Role-Based Access Control (RBAC);
- **Impact:** Full takeover of network functions, disruption of slice operations, unauthorised reconfiguration of slices, or insertion of malicious payloads affecting multiple tenants.

Weak access controls and inadequate privilege separation expose critical administrative functions to manipulation, undermining slice isolation and enabling attackers to move laterally across the network with elevated permissions.

4.3 Impact on Isolation and Derived Security Requirements

Given the multi-tenant and virtualised nature of 5G slicing, this section evaluates how different attack types compromise isolation guarantees and assesses their severity to inform the definition of security requirements.

The severity of each attack was assigned on a scale from 0 to 10, combining the impact on core security properties (Confidentiality, Integrity, and Availability (CIA)) with a quantitatively weighted contribution from the attack vector. The weighting scheme was defined to reflect the specific security priorities of 5G network slicing environments, where service disruption, cross-slice propagation, and shared resource contention make availability particularly relevant in the overall severity assessment.

The individual CIA values assigned to each attack were derived from a qualitative assessment informed by the literature review and complemented by analytical judgement regarding the expected effects of each attack on confidentiality, integrity, and availability within slicing architectures. Attack complexity is retained qualitatively to support

mitigation prioritisation without introducing unnecessary complexity into the numerical model.

1. **Impact on Fundamental Security Properties (CIA):** Each attack was evaluated according to its effect on:
   - *Confidentiality (C):* 0 (no impact) to 10 (critical exposure).
   - *Integrity (I):* 0 (no impact) to 10 (complete compromise).
   - *Availability (A):* 0 (no impact) to 10 (total interruption).
2. **Exploitability Attributes:**
   - *Attack Vector (V):* Remote, Local, or Insider, indicating required access. For the numerical component: Remote = 10, Local = 6, Insider = 8.
   - *Attack Complexity:* Low, Medium, or High (qualitative only, not included numerically).
3. **Severity Calculation (numerical, CIA + vector):**

$$\text{Severity (0–10)} = \frac{\alpha C + \beta I + \gamma A + \epsilon V}{\alpha + \beta + \gamma + \epsilon} \quad \text{with} \quad \alpha = 2,\ \beta = 1,\ \gamma = 10,\ \epsilon = 30.$$

   This weighting emphasises availability (propagation across slices) and the practical leverage of remote vectors in multi-slice environments.
4. **Example of Application:** For a *Slice Flooding via Orchestrator Overload* attack with $C = 0$, $I = 0$, $A = 9$, Remote vector ($V = 10$):

$$\text{Severity} = \frac{(2 \cdot 0) + (1 \cdot 0) + (10 \cdot 9) + (30 \cdot 10)}{2 + 1 + 10 + 30} = \frac{390}{43} \approx 9.07.$$

   Thus, severity is **9.07** (high).

Visual Representation of Severity

- **Low (0–3.99):** light green
- **Medium (4–6.99):** light yellow

- **High (7–10):** light red

Table 4.2: CIA impact and severity scoring of selected 5G slicing attack vectors

Attack	**Impact (CIA)**	**Attack Vector**	**Complexity**	**Severity (0–10)**
Slice Flooding via Orchestrator Overload	C: 0, I: 0, A: 9	Remote	Low	9.07
Misconfiguration Exploitation in Slice Deployment	C: 4, I: 6, A: 3	Remote	Medium	8.00
unauthorised Slice Modification via API Abuse	C: 2, I: 7, A: 3	Remote	Medium	7.93
Hypervisor Escape Leading to Cross-Slice Compromise	C: 3, I: 8, A: 6	Local	High	5.91
Targeted Hardware-Induced DoS Affecting All Slices	C: 1, I: 2, A: 9	Local	High	6.37
unauthorised Data Access via Shared Routing or Misconfigured Interfaces	C: 7, I: 6, A: 2	Remote	Medium	7.91
Cross-Slice Resource Exhaustion (CPU or Bandwidth Contention)	C: 1, I: 2, A: 8	Remote	Medium	8.93
Passive Traffic Sniffing Across Slices	C: 6, I: 3, A: 1	Remote	Medium	7.56
unauthorised Command Injection into Slice Control Functions	C: 2, I: 8, A: 4	Remote	Medium	8.19

The methodological revision presented above clarifies the interpretation of severity scores and ensures that risk treatment decisions account for both the magnitude of CIA impact and the practical exploitability reflected qualitatively by vector and complexity attributes.

Most attacks affecting slice isolation or orchestration components obtained scores above 7, highlighting the systemic nature of these threats and supporting the need for stronger isolation and access control mechanisms across the slicing infrastructure.

4.4 Summary

This chapter presented a structured vulnerability analysis across the 5G slicing architecture, linking theoretical threat models to practical attack scenarios. By quantifying the severity of each threat based on its impact and exploitability, the analysis provided a comprehensive view of how slice isolation can be compromised at different layers. These findings form the basis for the next chapter 5, which introduces a security framework addressing the identified weaknesses and proposing mitigation strategies for enhanced slice isolation.

Chapter 5

Conceptual Framework for Security Solutions

Building upon the risk assessment and severity analysis presented in Chapter 4, this chapter introduces a conceptual framework designed to strengthen security and isolation in 5G network slicing environments. While the previous chapter identified critical vulnerabilities and quantified their potential impact across architectural layers, the current section translates those findings into a structured, multi-layered security architecture.

The proposed framework integrates mechanisms for isolation enforcement, continuous monitoring, and automated response, addressing both the static and dynamic aspects of slice security. It aims to provide a holistic perspective—covering orchestration, virtualisation, communication, and management components—ensuring that each layer contributes to the overall resilience of the slicing environment. Rather than presenting an implementation blueprint, this framework serves as a theoretical foundation that can guide the design and validation of secure slicing platforms in future experimental or industrial contexts.

The objectives of this chapter are therefore fourfold:

1. To define a comprehensive architecture that mitigates the vulnerabilities and attack vectors identified earlier;

2. To establish guiding security principles that underpin the design of isolation, detection, and response mechanisms;

3. To propose concrete mitigation measures mapped to each layer of the slicing taxon-

omy;

4. To conceptually validate the framework by demonstrating its consistency and coverage against known threat categories.

5.1 Design Principles and Objectives

The conceptual framework is founded upon several interdependent security principles that reflect both the unique requirements of 5G slicing and established best practices in network and cloud security. These principles aim to ensure that security mechanisms are not isolated per component but operate as part of an integrated and adaptive defence model.

Defence-in-Depth

Security must be enforced across multiple layers of the 5G slicing architecture—from orchestration to the data plane—so that the compromise of a single component does not propagate to other domains. Each architectural layer introduces independent controls such as access validation, encryption, resource isolation, and anomaly detection, ensuring redundancy in protection.

Zero-Trust Slicing

Given the dynamic and multi-tenant nature of slicing, no entity, slice, or network function should be inherently trusted. Authentication, authorisation, and continuous verification is required for every interaction between orchestrators, VNFs, and user-plane components. This principle supports fine-grained access control and minimizes the risk of lateral movement between slices.

Adaptive and Automated Security

Static security policies are insufficient to counter evolving 5G threats. The framework therefore embeds automation and intelligence within orchestration and monitoring systems, enabling dynamic adaptation to detected anomalies. Machine learning techniques and rule-

based automation can assist in detecting deviations from normal behaviour and triggering corrective actions such as policy rollback, slice quarantine, or traffic rerouting.

Isolation by Design

Isolation must be treated as a core architectural property rather than a by-product of virtualisation. The framework promotes explicit isolation controls—including hardware-assisted virtualisation, slice-level quotas, and strict resource scheduling—to prevent contention and interference between tenants.

Compliance and Standard Alignment

To ensure interoperability, regulatory compliance, and future adoption, the proposed security measures align with recognized standards and frameworks such as 3rd Generation Partnership Project Service and System Aspects Working Group 5 (3GPP SA5), ETSI NFV-MANO, and National Institute of Standards and Technology (NIST) SP 800-207 for Zero Trust Architectures. In addition to these technical standards, the framework also considers the European regulatory landscape, particularly the Network and Information Security Directive 2 (EU 2022/2555) (NIS2) Directive[1], which defines cybersecurity and risk management obligations for essential and digital service providers, including telecommunications operators. Furthermore, the recommendations outlined in the European Union Agency for Cybersecurity (ENISA) 5G Security Toolbox are incorporated to ensure alignment with the European Union (EU)'s strategic approach to mitigating risks in 5G networks.

The alignment with these standards is reflected in several aspects of the proposed framework. At the orchestration and management layer, the structure and interfaces follow the functional model defined by 3GPP SA5 and the ETSI NFV-MANO reference architecture, ensuring interoperability between virtualised network functions and management entities. The adoption of Zero Trust principles from NIST SP 800-207 underpins the framework's authentication, authorisation, and segmentation mechanisms. In parallel, compliance with the NIS2 Directive is ensured through the integration of continuous monitoring, incident reporting, and risk assessment procedures. Finally, the inclusion of the ENISA 5G Security

[1] `https://www.cncs.gov.pt/pt/diretiva-sri-2-nis-2/`

Toolbox guidelines ensures that the proposed mitigations address the high-priority threat scenarios identified for European 5G deployments.

To substantiate this alignment, Table 5.1 provides a structured mapping between the framework's security mechanisms and the corresponding requirements defined across major standardisation and regulatory references. This comparison highlights how each control embodies specific obligations or recommendations from 3GPP SA5, ETSI NFV-MANO, NIST SP 800-207, the NIS2 Directive, and the ENISA 5G Security Toolbox, thereby reinforcing the framework's coherence with established industry and policy guidelines.

Table 5.1: Mapping of security mechanisms across 5G standards and frameworks

Framework Mechanism	**3GPP SA5 (OAM Management)**	**ETSI NFV-MANO**	**NIST SP 800-207 (Zero Trust)**	**NIS2 (Requirements)**	**ENISA 5G Security Toolbox**
Identity assurance; MFA; OAM federation	OAM access control; NRM inventory	Auth policies; SOL API security	Continuous identity checks; "never trust" principle	Identity and access governance	Credential and access control
Micro-segmentation; ABAC policies	Slice profiles; domain separation	Isolation via VIM/VNFM/ Orchestrator; connectivity rules	Attribute-based policies; dynamic decisions	Segmentation; access control requirements	Segmentation; lateral movement mitigation
Slice isolation; firewalling	Slice lifecycle; isolation KPIs	NS/NSD isolation constraints; forwarding domains	Micro-perimeters; trust plane separation	Network security and resilience requirements	Virtualisation risk mitigation
API hardening (mTLS, rate limiting, authz)	Secure OAM/service interfaces	SOL API logging, auth and integrity	PEP/PDP; least-privilege enforcement	Policy enforcement; monitoring and logging	API exposure limitation
Telemetry; logging; anomaly detection	FM/PM alarms and metrics	Observability; lifecycle events; VNF/NS metrics	Continuous monitoring and analytics	Logging, traceability and incident monitoring	SOC monitoring and threat detection

Framework Mechanism	**3GPP SA5 (OAM Management)**	**ETSI NFV-MANO**	**NIST SP 800-207 (Zero Trust)**	**NIS2 (Requirements)**	**ENISA 5G Security Toolbox**
Vulnerability management; patching	Change management; maintenance windows	VNF/VM/ container updates; catalog updates	Secure baselines; continuous remediation	Vulnerability remediation obligations	Component hardening; remediation
Image integrity; supply-chain assurance	Artifact validation; version compliance	Signed onboarding; trusted catalogs	Trust verification; attestation	Supply-chain assurance and supplier controls	Supplier vetting; supply-chain risk
Config compliance; drift control	CM/NRM auditing and consistency checks	Declarative NS/NSD compliance policies	Policy-as-code; continuous validation	Governance; accountability; configuration control	Secure configuration validation
Incident response; reporting	Rollback; FM/PM correlation	Automation for scaling, redeploy and isolation	Risk-based containment; response playbooks	Incident reporting and preparedness	Coordinated response workflows
Business continuity; disaster recovery (BC/DR)	Slice-level redundancy and resilience	Multi-site orchestration; backups	Control/data-plane resilience	Operational continuity and resilience measures	Service continuity measures

Together, this multidimensional alignment strengthens, both the theoretical validity and the practical applicability of the framework, ensuring coherence with emerging industry and regulatory practices.

Building on this foundation, the proposed principles support a layered security model that integrates prevention, detection, and response capabilities. The following sections translate these principles into an architectural design that operationalizes them across the four layers defined in the vulnerability taxonomy—Orchestration and Management, virtualisation, Network, and Interface and Communication.

5.2 Framework Architecture Overview

The proposed conceptual framework integrates multiple security mechanisms across the architectural layers of 5G network slicing. It builds upon the principles outlined in Section 5.1, combining preventive and adaptive measures to protect against the vulnerabilities identified in Chapter 4. The architecture adopts a layered design that mirrors the structure of the slicing taxonomy—Orchestration and Management, virtualisation, Network, and Interface and Communication—while introducing an overarching Monitoring and Response layer that operates across all domains.

The framework is structured around three core functional domains:

- **Preventive Controls:** static mechanisms that ensure isolation, access control, and secure configuration at each architectural layer;
- **Monitoring and Detection:** continuous collection and correlation of telemetry data to identify deviations from normal operational behaviour;
- **Automated Response and Recovery:** adaptive mechanisms capable of isolating compromised slices, revoking credentials, or reconfiguring orchestration policies in real time.

These domains interact in a feedback loop, enabling proactive and reactive security management. Figure 5.1 provides a visual representation of the framework, showing how security mechanisms are distributed across layers and how monitoring and response functions interconnect them to maintain global resilience.

The framework operates in a closed control loop. Each layer enforces its own set of preventive controls, while telemetry data from orchestrators, hypervisors, and network functions are continuously collected and analysed. When anomalies are detected—such as abnormal slice creation rates, inter-slice traffic leakage, or excessive resource contention—the Monitoring and Response layer activates predefined mitigation routines. These include temporary isolation of affected slices, reallocation of virtualised resources, and enforcement of stricter access control rules.

Through this design, the framework achieves three complementary goals:

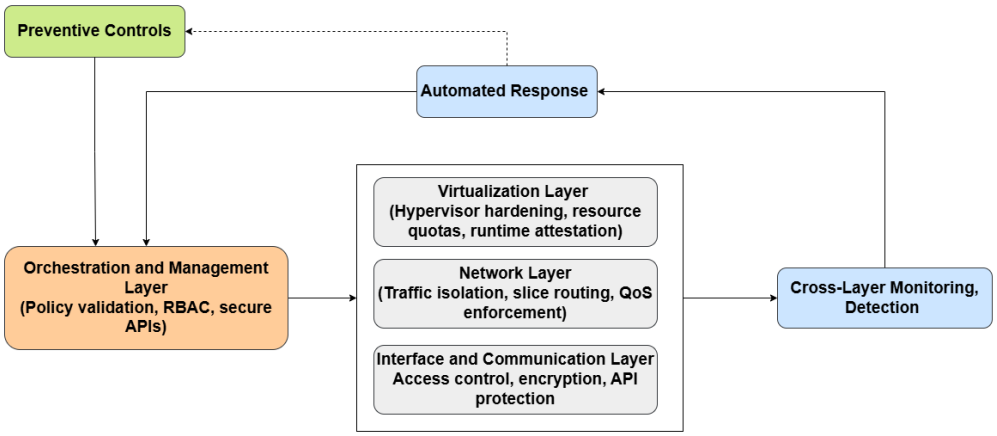

Figure 5.1: Feedback-driven security architecture for 5G network slicing

1. **Isolation Assurance:** maintaining logical and physical separation of slice resources under both normal and stressed conditions;

2. **Continuous Trust Verification:** dynamically validating the integrity and behaviour of components across all layers;

3. **Resilient Recovery:** enabling automated containment and restoration actions that minimise the impact of detected intrusions.

The next section expands upon this architecture by mapping the proposed security mechanisms to the specific layers of the slicing taxonomy, illustrating how each component contributes to mitigating the vulnerabilities and attack vectors previously identified.

5.3 Security Mechanisms per Layer

This section details the specific security mechanisms proposed for each architectural layer of the 5G slicing framework. Each group of mechanisms directly addresses the vulnerabilities and attack vectors identified in Chapter 4, providing preventive, detective, and responsive controls aligned with the principles of isolation, automation, and continuous trust verification.

5.3.1 Orchestration and Management Layer

The orchestration layer is responsible for slice creation, scaling, and lifecycle management, making it a primary target for attacks such as API abuse, misconfiguration, and orchestrator overload. Security at this layer must therefore focus on protecting control-plane functions and ensuring policy consistency throughout the slice deployment process.

Proposed mechanisms:

- **API Hardening and Authentication:** enforce strict access control on orchestration APIs using mutual Transport Layer Security (TLS), token-based authentication, and per-tenant rate limiting;
- **Policy Validation and Configuration Consistency:** implement automated validation of NSD/VNFD templates to prevent deployment of misconfigured slices or insecure parameter overrides;
- **RBAC:** define fine-grained user and service roles, limiting access to slice management functions and preventing privilege escalation;
- **Audit Logging and Traceability:** maintain secure, immutable logs of orchestration operations to enable forensic analysis and anomaly detection;
- **Dynamic Load and Request Throttling:** prevent orchestrator flooding by regulating the rate of slice creation and scaling requests.

Together, these mechanisms mitigate risks associated with the attacks described in the orchestration domain—namely Slice Flooding via Orchestrator Overload, Misconfiguration Exploitation, and API Abuse.

5.3.2 Virtualisation Layer

The virtualisation layer hosts network functions and enables resource abstraction through hypervisors and container runtimes. Weaknesses in this domain can compromise multiple slices simultaneously, as shown by attacks such as Hypervisor Escape and Cross-Slice Resource Exhaustion. The proposed controls strengthen both resource isolation and the integrity of the execution environment.

Proposed mechanisms:

- **Hypervisor and Container Hardening:** adopt security baselines (e.g., KVM/QEMU hardening, SELinux/AppArmor enforcement, minimal image builds);
- **Hardware-Assisted virtualisation:** leverage VT-x, AMD-V, or ARM TrustZone to ensure strict separation between guest and host environments;
- **Slice-Level Resource Quotas:** apply CPU, memory, and bandwidth quotas per slice to prevent contention and denial-of-service propagation;
- **Runtime Integrity Verification:** monitor system calls, process integrity, and kernel modules to detect unauthorised modifications;
- **Secure Image and Descriptor Management:** validate VNFs and container images before deployment through checksum and signature verification.

In addition to signature-based verification, cryptographic hash mechanisms (e.g., SHA-256 or SHA-3) should be computed and validated for all VNF/Cloud-Native Network Function (CNF) images, descriptor packages, and dependency artifacts. These hashes ensure that onboarding artifacts have not been tampered with, provide strong integrity guarantees during storage and transfer, and enable the orchestrator to detect unauthorised modifications or supply-chain manipulation before deployment.

These measures ensure that even if a single VNF or virtual machine is compromised, the attacker's ability to move laterally or exhaust shared resources remains limited.

5.3.3 Network Layer

The network layer governs inter-slice communication, routing, and traffic enforcement. As demonstrated by the Cross-Slice Resource Exhaustion and unauthorised Data Access scenarios, weak segmentation or shared transport functions can expose slices to lateral interference. Security mechanisms here must enforce both data-plane and control-plane isolation.

Proposed mechanisms:

- **Traffic Segmentation and VLAN Enforcement:** apply strict VLAN or Virtual Extensible Local Area Network (VXLAN) tagging for slice traffic to prevent cross-slice leakage;

- **Micro-Segmentation Policies:** enforce slice-specific routing tables and ACLs across SDN controllers and virtual switches;
- **Encrypted Intra-Slice Communication:** use IPsec or TLS tunnels between VNFs to protect control and user-plane data flows;
- **QoS and Rate Limiting:** maintain traffic fairness by assigning bandwidth guarantees and ceilings per slice;
- **Network Telemetry Integration:** continuously monitor latency, packet drops, and abnormal flow patterns to detect isolation breaches.

The combination of segmentation, encryption, and telemetry provides both preventive and detective assurance that each slice operates within defined communication boundaries.

5.3.4 Interface and Communication Layer

This layer represents the external-facing interfaces that connect user equipment, APIs, and administrative portals to the slicing infrastructure. It is exposed to a wide range of attacks—such as Passive Traffic Sniffing or unauthorised Command Injection that can compromise confidentiality and control functions. The proposed controls focus on protecting data exchange, enforcing strong authentication, and preventing injection or eavesdropping.

Proposed mechanisms:

- **Secure Protocols and Encryption:** enforce TLS 1.3 and certificate pinning across all northbound and southbound APIs, as well as user-plane interfaces;
- **API Gateway Security:** implement request sanitization, input validation, and anomaly-based filtering to prevent injection attacks;
- **Multi-Factor and Mutual Authentication:** strengthen administrative and orchestration interfaces against credential theft or misuse;
- **Secure Logging and Telemetry Channels:** ensure that monitoring data cannot be intercepted or tampered with during transmission;

- **Continuous Vulnerability Scanning:** integrate API and interface scanning tools (e.g., Open Worldwide Application Security Project (OWASP) Zed Attack Proxy (ZAP), OpenVAS) into the orchestration workflow.

Through these mechanisms, the interface and communication layer provides a secure boundary between the slicing platform and external entities, ensuring that only authorized and validated communications occur.

In summary, each architectural layer contributes complementary controls that together uphold the principles of defence-in-depth and zero-trust operation. The following section 5.4 extends this design by introducing the cross-layer monitoring and automated response mechanisms that operationalize real-time protection and adaptive resilience.

5.4 Monitoring, Detection, and Automated Response

Effective protection in 5G network slicing cannot rely solely on preventive controls. Given the dynamic, distributed, and multi-tenant nature of the slicing environment, continuous monitoring and adaptive response mechanisms are essential to detect anomalies, contain incidents, and restore operational stability in real time. This section describes the cross-layer monitoring and automated response system integrated within the proposed conceptual framework.

5.4.1 Cross-Layer Monitoring Architecture

The monitoring subsystem operates across all architectural layers—from orchestration to communication interfaces—collecting and correlating telemetry data in a unified analytics pipeline. Each component (e.g., orchestrator, hypervisor, SDN controller) produces events and metrics that feed into a central Security Data Lake, where they are normalized and analysed for behavioural deviations.

Key monitoring components:

- **Telemetry Agents:** lightweight probes embedded within VNFs, hypervisors, and APIs that collect logs, resource metrics, and flow statistics;

- **Event Correlation Engine:** aggregates data from different sources to identify multi-layer anomalies (e.g., abnormal slice creation rate combined with traffic bursts);
- **AI/ML-Based Anomaly Detection:** employs machine learning models—such as clustering, autoencoders, or statistical baselines—to detect deviations from expected slice behaviour;
- **Security Information and Event Management (SIEM):** provides centralized visualization, alerting, and policy feedback for orchestrator-driven actions.

This distributed monitoring approach ensures both vertical visibility (from physical to application layer) and horizontal correlation across slices, enabling early detection of multi-domain attacks.

5.4.2 Anomaly Detection and Classification

Detected anomalies are automatically classified according to their scope and severity, based on a rule-based engine aligned with the taxonomy defined in Chapter 4.1. The classification differentiates between:

- **Performance Anomalies:** symptoms of resource exhaustion or congestion (e.g., cross-slice CPU contention);
- **Configuration Anomalies:** deviations from approved NSD/VNFD descriptors or orchestration policies;
- **Security Incidents:** events indicating potential compromise, such as unauthorised API calls, policy violations, or data leakage.

Each class of anomaly triggers a predefined response policy with associated mitigation actions. For instance, resource contention may result in temporary throttling or migration of VNFs, while unauthorised slice modifications trigger automatic rollback and credential revocation.

5.4.3 Automated Response Mechanisms

The response layer implements a closed control loop that enables autonomous mitigation and recovery actions without human intervention. These actions are orchestrated by

the Security Orchestrator, which interfaces with the MANO stack to enforce policy changes dynamically.

Response capabilities:

- **Slice Quarantine:** isolate the affected slice or VNF by revoking network access and suspending orchestration operations until integrity verification is complete;
- **Policy Rollback:** revert to the last known secure configuration in case of detected misconfiguration or policy deviation;
- **Resource Reallocation:** dynamically migrate VNFs or redistribute workloads to maintain service continuity during localized incidents;
- **Credential and Session Revocation:** immediately invalidate access tokens, certificates, or credentials linked to compromised entities;
- **Automated Incident Reporting:** generate standardized alerts (e.g., Structured Threat Information Expression (STIX)/Trusted Automated Exchange of Intelligence Information (TAXII) formats) for external Security Operations Center (SOC) or Computer Security Incident Response Team (CSIRT) integration.

Through the combination of detection and automated mitigation, the framework achieves a high degree of resilience, minimizing the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to incidents.

5.4.4 Integration with Orchestration and Policy Feedback

The monitoring and response mechanisms operate in coordination with the orchestration layer to support adaptive security governance. Detected events and response outcomes are continuously fed back into the orchestration policies, enabling the system to learn and adjust thresholds or reaction strategies over time. This self-adaptive loop ensures that the slicing platform evolves in response to changing operational conditions and emerging threat patterns.

Formally, this integration can be represented as a continuous feedback cycle where each stage reinforces the next, forming a dynamic defence mechanism that aligns with modern zero-trust and autonomous networking paradigms. 5.1

In summary, the monitoring and automated response subsystem transforms the proposed framework from a static set of defences into a living, adaptive security model. By maintaining persistent situational awareness and enabling policy-driven mitigation, it ensures that slice isolation, integrity, and availability are preserved even under active attack conditions.

5.5 Theoretical Validation

Although the proposed framework has not been implemented or empirically tested, its validity can be established through a structured theoretical analysis. This validation assesses whether the framework provides adequate coverage against the vulnerabilities and attack vectors identified in Chapter 4, ensuring conceptual soundness, consistency, and completeness.

The analysis follows two complementary perspectives:

1. **Coverage Validation:** verifying that each category of threat defined in the vulnerability taxonomy is addressed by at least one mitigation mechanism and one adaptive control;

2. **Consistency Validation:** ensuring that mechanisms do not introduce contradictions or dependencies that could weaken isolation or automation objectives.

To support this process, Table 5.2 presents a mapping between the representative attack scenarios and the security mechanisms proposed in the framework. The table illustrates how each attack vector is mitigated by preventive, detective, and responsive measures operating across different layers.

Table 5.2: Mitigation mechanisms applied to representative cross-slice attack scenarios

Attack Scenario	**Primary Mitigation Mechanisms**	**Layer(s) Involved**
Slice Flooding via Orchestrator Overload	Rate limiting, request throttling, API authentication, load balancing of orchestration services	Orchestration and Management
Misconfiguration Exploitation in Slice Deployment	Policy validation, NSD/VNFD template verification, configuration consistency checks	Orchestration and Management
Unauthorised Slice Modification via API Abuse	RBAC enforcement, mutual TLS, audit logging, token-based access control	Orchestration and Management, Interface
Hypervisor Escape Leading to Cross-Slice Compromise	Hypervisor hardening, hardware-assisted virtualisation, runtime integrity verification	Virtualisation
Targeted Hardware-Induced DoS Affecting All Slices	Resource quotas, hardware-level monitoring, adaptive VNF migration, redundancy mechanisms	Virtualisation, Monitoring
Unauthorised Data Access via Shared Routing or Misconfigured Interfaces	Traffic segmentation (VLAN/VXLAN), SDN micro-segmentation, encrypted intra-slice communication	Network
Cross-Slice Resource Exhaustion (CPU or Bandwidth Contention)	Slice-level quotas, dynamic resource allocation, anomaly-based performance monitoring	Virtualisation, Network

Attack Scenario	**Primary Mitigation Mechanisms**	**Layer(s) Involved**
Passive Traffic Sniffing Across Slices	TLS/IPsec enforcement, secure logging, interface-level telemetry auditing	Interface and Communication, Network
Unauthorised Command Injection into Slice Control Functions	Input validation, API gateway filtering, multi-factor authentication, credential revocation on detection	Interface and Communication, Orchestration

5.5.1 Coverage and Consistency Analysis

The mapping in Table 5.2 confirms that each major attack scenario is mitigated by at least one control within the relevant architectural layer, complemented by detection and automated response mechanisms. For example, control-plane attacks such as unauthorised Slice Modification are countered through strict API authentication, while data-plane threats such as Passive Traffic Sniffing are mitigated through encryption and interface monitoring.

Coverage validation:

- All nine representative attacks identified in Chapter 4 are addressed by multiple defences spanning preventive, detective, and responsive domains;
- Cross-layer coverage is achieved by design, ensuring that anomalies undetected at the orchestration level can still be captured through telemetry or integrity checks at lower layers;
- The Monitoring and Response subsystem acts as a global control loop, maintaining adaptive protection across the full taxonomy of vulnerabilities.

Consistency validation: The interactions among security controls were conceptually verified to avoid conflicts between automation and enforcement logic. For instance, automated rollback and quarantine procedures are triggered only after detection thresholds are confirmed through multi-source telemetry correlation, preventing false positives

from causing unnecessary service interruptions. Furthermore, access control, isolation, and monitoring mechanisms operate independently, maintaining modularity and reducing the risk of cascading failures.

5.5.2 Formal Coherence of the Framework

Formally, the framework satisfies three core security invariants derived from the CIA triad and the principle of continuous verification:

1. **Isolation Invariant (I_s):** no unauthorised communication or resource sharing occurs between slices under defined orchestration and virtualisation policies;
2. **Integrity Invariant (I_i):** all configuration and control operations are authenticated, verified, and traceable through immutable logging mechanisms;
3. **Availability Invariant (I_a):** the system preserves service continuity by reallocating or isolating resources under stress or attack conditions.

Theoretical validation demonstrates that the framework upholds these invariants across all four layers of the slicing architecture. Hence, even in the absence of empirical deployment, the conceptual consistency and multi-layer redundancy of the framework substantiate its robustness against the main classes of attacks previously identified.

In conclusion, the proposed conceptual framework provides comprehensive theoretical coverage and maintains internal coherence with the vulnerability taxonomy and severity analysis. It offers a consistent, formally grounded security model capable of addressing isolation, integrity, and availability challenges in multi-tenant 5G slicing environments. The following chapter builds upon these findings to discuss the broader implications, limitations, and potential extensions of this dissertation.

5.6 Summary

This chapter presented a conceptual framework designed to enhance security and isolation in 5G network slicing environments. Building upon the vulnerability taxonomy and risk assessment developed in Chapter 4, the framework consolidates preventive, detective, and responsive controls into a unified, multi-layered architecture.

The proposed model introduces five guiding principles—defence-in-depth, zero-trust slicing, adaptive automation, isolation by design, and standards compliance—that collectively shape a resilient security posture. Each architectural layer of the slicing ecosystem—Orchestration and Management, virtualisation, Network, and Interface and Communication—was associated with specific mechanisms that address both direct vulnerabilities and inter-slice propagation risks.

Furthermore, the framework incorporates a continuous monitoring and automated response subsystem capable of detecting anomalies, triggering corrective actions, and reinforcing policy adaptation in real time. This dynamic feedback loop transforms the framework into an adaptive, self-correcting security model that evolves with the operational state of the network.

The theoretical validation confirmed that the framework provides full coverage across the previously identified attack vectors, maintaining formal coherence with the core security invariants of isolation, integrity, and availability. By demonstrating conceptual robustness and internal consistency, the framework establishes a foundation for future experimental validation and for the development of secure orchestration mechanisms in real 5G slicing environments.

The next chapter discusses the implications of these findings, highlighting the contributions, limitations, and prospective directions for extending this dissertation into practical implementations and policy design.

Chapter 6

Analysis and Discussion of Results

This chapter presents a critical discussion of the results obtained from the vulnerability assessment and conceptual framework developed in the previous chapters. While Chapter 4 systematically identified vulnerabilities and quantified their impact on slice isolation, Chapter 5 proposed a theoretical security framework aimed at mitigating those risks through layered and adaptive mechanisms.

The purpose of this discussion is to interpret these findings in the broader context of 5G security research and to evaluate the theoretical contribution of the proposed framework in addressing the most critical weaknesses identified across the slicing architecture. Rather than restating the results, this chapter analyses their implications, coherence, and alignment with the principles of multi-tenancy, virtualisation, and orchestration in 5G systems.

The discussion proceeds as follows: Section 6.1 synthesizes the main findings from the vulnerability analysis and risk evaluation; Section 6.2 interprets the conceptual framework as a response to those weaknesses; Section 6.3 compares the proposed approach with the current state of the art; and Section 6.4 reflects on the implications and limitations of the research. The chapter concludes with a summary in Section 6.5, preparing the transition to the final conclusions of this dissertation.

6.1 Synthesis of Findings from the Vulnerability Analysis

The vulnerability and risk analysis presented in Chapter 4 revealed that the majority of high-severity threats originate from the Orchestration and Management Layer and the Virtualisation Layer. These layers exhibited systemic weaknesses due to their central role in resource allocation, slice lifecycle management, and cross-slice dependency control. In contrast, vulnerabilities in the Network Layer and Interface and Communication Layers tended to be more localized but could still propagate laterally under specific misconfiguration conditions.

The severity assessment demonstrated that over half of the analysed attacks reached scores above 7, indicating high-impact scenarios with potential cross-slice effects. Examples include the Slice Flooding via Orchestrator Overload, which exposes the orchestration layer to denial-of-service conditions, and the Hypervisor Escape Leading to Cross-Slice Compromise, capable of breaching isolation at the virtualisation layer. These results confirm that the most critical vulnerabilities are not limited to isolated functions but rather stem from shared control and management components that lack robust isolation and segmentation guarantees.

A recurrent finding across all categories was the dual nature of misconfiguration and shared resource exploitation. Attacks such as the Misconfiguration Exploitation in Slice Deployment and the unauthorised Slice Modification via API Abuse highlight how orchestration systems remain highly dependent on human and procedural accuracy. These vulnerabilities often arise not from novel exploits but from insufficient enforcement of configuration integrity, input validation, and policy consistency.

Furthermore, the results underscore the interdependence between availability and confidentiality threats: attacks targeting resource exhaustion, such as Cross-Slice Resource Exhaustion, can indirectly degrade monitoring or isolation services, thereby facilitating unauthorised access or data leakage. This relationship suggests that in multi-slice environments, the boundaries between traditional CIA properties are blurred—availability failures can lead to breaches of confidentiality and integrity.

Overall, the analysis supports the conclusion that existing open-source 5G slicing platforms provide only partial enforcement of isolation, particularly in orchestration and vir-

tualisation layers. The combination of weak policy enforcement, shared execution environments, and inadequate runtime monitoring amplifies the risk of cascading failures. These insights provide the foundation for the conceptual security framework proposed in Chapter 5, which addresses these systemic gaps through defence-in-depth, automation, and adaptive isolation mechanisms.

6.2 Interpretation of the Conceptual Framework

The conceptual framework introduced in Chapter 5 was designed as a theoretical response to the vulnerabilities and systemic risks identified in the previous analysis. Its structure reflects the multi-layered nature of 5G slicing, combining prevention, detection, and response mechanisms under a unified security model. This section interprets the framework's effectiveness and internal coherence in mitigating the weaknesses observed across orchestration, virtualisation, network, and communication layers.

At a conceptual level, the framework demonstrates a strong correspondence between the taxonomy of threats and the placement of mitigation mechanisms. For instance, the inclusion of isolation-by-design controls directly addresses the cross-slice interference and resource exhaustion issues identified in the virtualisation and Network Layers. Similarly, the emphasis on zero-trust slicing and continuous verification mechanisms provides a structured countermeasure to authentication and authorisation weaknesses prevalent in orchestration and management interfaces.

A key strength of the framework lies in its layered design principle, where each architectural domain enforces independent but interoperable controls. This defence-in-depth approach ensures that the compromise of one component—such as an exposed API or a vulnerable VNF—does not automatically propagate to other domains. By distributing control across multiple layers and integrating monitoring feedback loops, the framework enhances resilience against both direct attacks and cascading failures.

The integration of adaptive and automated security functions also represents a theoretical advancement compared to static policy-based models. Traditional approaches to 5G security rely heavily on predefined policies that fail to react to dynamic operational states. In contrast, the proposed model embeds automated response mechanisms capable

of adjusting orchestration policies in real time—such as throttling slice requests, isolating compromised functions, or rolling back misconfigurations detected through anomaly monitoring. This transforms the framework from a purely preventive system into an adaptive and self-correcting architecture.

Furthermore, the conceptual alignment with existing standards—such as 3GPP SA5, ETSI NFV-MANO, and NIST's Zero Trust Architecture (SP 800-207)—provides theoretical validity and ensures compatibility with future developments in slicing orchestration. This alignment reinforces the practical relevance of the framework, positioning it as a reference model rather than an isolated academic construct.

Overall, the interpretation confirms that the framework effectively maps the theoretical vulnerabilities identified in Chapter 4 to concrete mitigation principles. Its strength resides not only in addressing individual attack vectors but also in redefining isolation as a continuously monitored and dynamically enforced process. By merging zero-trust design, adaptive automation, and formal layer separation, the framework establishes a coherent foundation for secure and resilient 5G slicing architectures.

6.3 Comparative Discussion with State of the Art

To contextualize the theoretical contribution of the proposed framework, it is essential to compare its structure and guiding principles with existing approaches to 5G slicing security presented in recent literature and standards. Although a considerable body of work between 2021 and 2024 has examined topics such as AI-assisted orchestration, zero-trust network design, and virtualisation hardening, very few studies provide an integrated model that explicitly links threat taxonomy, risk quantification, and mitigation logic. This section discusses how the proposed framework aligns with, extends, or complements these current research trends.

Recent contributions have increasingly explored the use of artificial intelligence and machine learning for dynamic slice management and anomaly detection. These approaches tend to emphasize predictive analysis and adaptive orchestration mechanisms. However, they often lack a formal connection between detected anomalies, the corresponding risk level, and the concrete security controls required to address them. In contrast, the frame-

work developed in this dissertation establishes an explicit mapping between vulnerabilities (as defined by the taxonomy), associated risk scores, and adaptive mitigation actions. This provides clear traceability and enables more structured and consistent decision-making in automated orchestration environments.

Another prominent research direction involves the adaptation of zero-trust principles to 5G slicing contexts. Existing models introduce continuous verification and fine-grained authentication techniques to reduce the attack surface in multi-tenant environments. While such approaches effectively strengthen access control and privilege management, they typically do not consider the operational interplay across orchestration, virtualisation, and communication layers. The framework proposed here expands the zero-trust paradigm by incorporating verification not only at the user or API level but also across orchestration workflows and inter-slice dependencies, ensuring that isolation policies remain enforceable even under frequent reconfiguration.

Parallel to this, several works have examined formal verification and policy-based enforcement as mechanisms to ensure slice isolation. These approaches provide strong guarantees for specific components but are often restricted to static configurations or validation of individual layers. The proposed model differs by combining formal invariants with runtime adaptability within a broader defence-in-depth strategy. By integrating both preventive and reactive dimensions, it bridges the gap between theoretical assurance and operational resilience.

When compared with widely used open-source implementations such as OSM and Open Network Automation Platform (ONAP), the proposed conceptual framework sheds light on the limitations of current orchestration stacks in enforcing fine-grained isolation and providing real-time anomaly response. Although these platforms implement essential security features—such as access control, logging, and authentication—they lack native mechanisms for cross-layer correlation, dynamic containment, or automated mitigation. The adaptive and multi-layered design introduced in this dissertation therefore offers a theoretical blueprint for enhancing these orchestration environments, aligning them with emerging 3GPP and ETSI recommendations on closed-loop security management.

In summary, although existing research and frameworks contribute meaningful insights into various dimensions of slicing security, they remain fragmented and often address iso-

lated functionalities. The framework proposed in this dissertation advances the state of the art by integrating three elements that are rarely combined in prior work:

- a threat-driven taxonomy that anchors the security architecture in realistic attack models;
- a formalized risk quantification method supporting prioritization and traceability;
- an adaptive orchestration layer capable of dynamic enforcement and automated response.

Together, these components position the proposed model as a comprehensive and theoretically consistent blueprint for secure and resilient network slicing.

6.4 Implications and Limitations

The results of this dissertation have both theoretical and practical implications for the design and governance of secure 5G slicing infrastructures. By formally connecting vulnerabilities, risk quantification, and mitigation principles, the proposed framework provides a conceptual foundation that can inform future implementations, policy guidelines, and standardization efforts in network security orchestration.

From a practical standpoint, the framework offers a structured approach for integrating security into the entire slice lifecycle—from instantiation and orchestration to monitoring and response. This perspective aligns with the evolution of 3GPP and ETSI standards, which increasingly emphasize the need for closed-loop and intent-based security management. The inclusion of adaptive response mechanisms and cross-layer monitoring could serve as a blueprint for enhancing open-source platforms such as OSM or ONAP, particularly in their handling of real-time anomaly detection and containment. In this regard, the conceptual model bridges the current gap between theoretical isolation requirements and their operational realization.

The framework also holds implications for regulatory and compliance contexts. By explicitly mapping attack vectors to confidentiality, integrity, and availability impacts, it facilitates risk assessment processes compatible with cybersecurity frameworks such

as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27005 and NIST SP 800-30. This traceability may support the development of auditable security models for multi-tenant network infrastructures, where isolation breaches can have cascading effects across services and domains.

Despite these contributions, several limitations must be acknowledged. First, the validation of the framework remains theoretical. Due to the technical instability of open-source slicing environments, empirical testing was not feasible within the scope of this dissertation. Consequently, the results rely on conceptual modelling and qualitative reasoning rather than on quantitative performance data. Future research should therefore focus on implementing the proposed architecture in controlled experimental environments—such as Free5GC or OSM testbeds—to evaluate its scalability, performance overhead, and detection accuracy under real network conditions.

Second, the framework's complexity poses challenges for integration into existing orchestration systems. Automated policy adaptation and cross-layer monitoring demand significant orchestration intelligence, which may introduce computational overhead or latency in dynamic slice environments. The balance between automation, responsiveness, and operational efficiency remains an open research question.

Despite these overhead considerations, it is important to emphasize that the additional latency and processing load introduced by the proposed framework remain moderate and proportional to the security benefits achieved. Continuous monitoring, adaptive enforcement, and automated containment inevitably require additional computational resources, but the resulting overhead is significantly outweighed by the reduction in the likelihood and impact of isolation breaches. In multi-tenant slicing environments, where cross-slice compromise may lead to cascading failures or large-scale service disruption, this trade-off is not only acceptable but essential. The framework therefore introduces a controlled and predictable cost that directly corresponds to a substantial increase in resilience and operational security.

Finally, while the framework addresses most known classes of vulnerabilities, it assumes a cooperative trust model between orchestration and infrastructure components. In highly adversarial or compromised scenarios—such as malicious hypervisors or insider threats with full administrative access—additional layers of assurance (e.g., hardware attestation,

trusted execution environments) may be required to preserve the security invariants.

In conclusion, the implications of this dissertation extend beyond academic analysis. The proposed framework outlines a pathway toward secure, adaptive and isolation-aware 5G slicing architectures, but its realization will depend on future empirical validation, optimization and standardization efforts. Recognizing its theoretical limitations while emphasizing its architectural potential ensures a balanced perspective that sets the stage for the concluding remarks in the next chapter.

6.5 Summary

This chapter provided a comprehensive discussion and interpretation of the results obtained throughout the research. By connecting the findings from the vulnerability assessment and the conceptual security framework, it established a coherent understanding of how theoretical analysis can inform the design of secure and isolation-aware 5G slicing architectures.

The synthesis of the vulnerability analysis confirmed that the most critical threats originate from the orchestration and virtualisation layers, where weak isolation, shared control mechanisms, and configuration inconsistencies expose the entire slicing ecosystem to systemic risks. These findings justified the need for an integrated security model capable of addressing both inter-slice dependencies and cross-layer propagation paths.

The interpretation of the conceptual framework demonstrated that a multi-layered, adaptive, and zero-trust architecture can effectively mitigate the identified weaknesses. Through the combination of defence-in-depth, continuous monitoring, and automated response, the framework promotes an operational paradigm in which isolation is maintained dynamically and verified continuously rather than statically assumed. Its theoretical alignment with established standards such as 3GPP, ETSI, and NIST further reinforces its conceptual soundness and applicability to future implementations.

The comparative analysis with current research positioned the framework as a comprehensive and innovative contribution that unifies threat taxonomy, risk quantification, and adaptive enforcement—three elements often treated independently in existing studies. While the approach remains theoretical, its structured design provides a foundation for

future experimental validation and integration into practical orchestration environments.

Finally, the discussion of implications and limitations highlighted both the potential impact and the boundaries of the proposed framework. Its scalability, automation logic, and performance efficiency must be empirically validated, yet its conceptual robustness already offers a valuable roadmap for advancing secure 5G slicing.

In summary, this chapter consolidated the analytical and theoretical components of the dissertation, demonstrating that the proposed framework successfully bridges the gap between vulnerability analysis and architectural mitigation. The following chapter concludes the study by summarizing its main contributions, identifying future research directions, and outlining the broader significance of this work for the evolution of secure network slicing.

Chapter 7

Conclusions and Future Work

This final chapter concludes the dissertation by summarizing the main findings, interpreting their significance in the context of 5G network slicing security, and outlining potential directions for future research. It reflects on how the theoretical analysis and conceptual framework developed throughout the study contribute to advancing the understanding of isolation and resilience in multi-tenant 5G environments. By consolidating the results and discussing their implications, this chapter provides both closure to the research and a foundation for subsequent empirical and theoretical developments in the field.

7.1 Summary of Findings

This dissertation investigated the security challenges and isolation weaknesses inherent to 5G network slicing architectures, focusing on how orchestration, virtualisation, and inter-slice dependencies shape the overall threat landscape. Through a structured, theory-driven approach, the study combined a detailed vulnerability taxonomy, a risk-based severity analysis, and the design of a conceptual security framework aimed at strengthening slice isolation.

The analysis conducted in Chapter 4 revealed that the most critical vulnerabilities arise from the orchestration and virtualisation layers, where weak control mechanisms, shared infrastructures, and misconfigurations undermine isolation guarantees. By developing a classification of threats aligned with 5G architectural layers, the research provided a systematic overview of how attacks may propagate across slices, compromising confi-

dentiality, integrity, and availability. The risk evaluation method introduced a weighted scoring model to quantify attack severity, demonstrating that most high-impact scenarios stem from insufficient resource segregation and poor policy enforcement.

Building upon these findings, Chapter 5 introduced a conceptual framework for security in network slicing. The model integrates defence-in-depth, zero-trust principles, adaptive monitoring, and automated response mechanisms to ensure dynamic and continuous enforcement of isolation. This architecture not only reflects the structural complexity of slicing environments but also aligns with emerging standards such as 3GPP SA5 and ETSI NFV-MANO. The comparative analysis in Chapter 6 further established the originality of the framework, highlighting its holistic approach to mapping vulnerabilities, quantifying risks, and proposing layered countermeasures. Overall, the research achieved its primary goal of defining a theoretically consistent foundation for secure and resilient 5G network slicing.

7.2 Conclusions

The research presented in this dissertation demonstrates that ensuring isolation in 5G network slicing requires more than static segmentation or access control. It demands a comprehensive and adaptive security model that continuously monitors, validates, and enforces separation between slices and management domains. The proposed conceptual framework embodies this principle by integrating proactive prevention with dynamic detection and automated mitigation, providing a balanced approach between theoretical rigor and practical applicability.

One of the key contributions of this work is the introduction of a cross-layer vulnerability taxonomy explicitly mapped to architectural layers of 5G slicing. This structure provides a clear analytical foundation for identifying where and how isolation failures may occur. The complementary risk assessment model quantifies the impact of these vulnerabilities, offering a transparent and reproducible method for prioritizing security measures. Together, these components create a coherent methodology for assessing and mitigating risks in complex, multi-tenant network environments.

The conceptual framework developed in this dissertation contributes to advancing the

state of the art by bridging the gap between theoretical vulnerability analysis and architectural mitigation design. Its integration of zero-trust principles, defence-in-depth strategies, and adaptive orchestration enables the construction of more resilient slicing infrastructures capable of resisting cascading failures and cross-slice exploitation. Although theoretical in nature, the framework establishes a solid foundation for future empirical validation and standardization.

In conclusion, this dissertation contributes a structured, theoretically validated model that enhances the understanding and management of security in network slicing. It provides both a conceptual reference for researchers and a potential design blueprint for developers and network operators aiming to build secure and adaptive 5G infrastructures.

7.3 Future Work

While this dissertation establishes a solid theoretical foundation, several avenues remain open for future exploration and validation. The most immediate next step involves the implementation and empirical evaluation of the proposed framework within controlled 5G testbeds. Platforms such as Free5GC, OSM, or ONAP could serve as experimental environments for testing the scalability, responsiveness, and interoperability of the proposed security mechanisms. Such implementations would also enable the quantification of performance overhead, detection accuracy, and recovery time, providing practical validation for the conceptual model.

Another promising direction concerns the integration of artificial intelligence and machine learning techniques to enhance adaptive orchestration. By incorporating predictive analytics or reinforcement learning, the framework could evolve into a self-optimizing security architecture capable of anticipating emerging threats and autonomously reconfiguring isolation policies in real time. This would reinforce its applicability to highly dynamic and autonomous 6G environments.

A complementary research path involves exploring distributed security mechanisms based on blockchain technologies. Smart contracts may be employed to enforce authentication, authorisation, and auditability across slices, enabling tamper-proof logging and verifiable cross-slice interactions. Such an approach could strengthen trust in multi-tenant

environments and provide decentralised guarantees for isolation enforcement.

Future work may also examine the impact of quantum computing on the cryptographic primitives currently used in slicing architectures. As quantum-capable adversaries could compromise widely deployed asymmetric algorithms, it becomes essential to assess the resilience of slice-to-slice communication and orchestration interfaces under post-quantum threat models. This includes the study of quantum-resistant key-exchange mechanisms and the integration of post-quantum cryptography into 5G and 6G management and control planes.

Additionally, the application of formal verification methods constitutes another opportunity for strengthening the guarantees offered by the proposed framework. Techniques such as temporal logic modelling, runtime verification, or model checking could be used to mathematically ensure that critical security invariants—such as resource separation and trust boundaries—remain preserved under specified operational conditions.

Finally, expanding the scope beyond 5G, the conceptual principles introduced here may be applied to next-generation network paradigms, including edge slicing, cloud-native infrastructures, and zero-touch network management. By validating and refining these ideas through experimental research and industry collaboration, this line of work can contribute to the development of more secure, intelligent, and adaptive communication infrastructures.

References

[1] Essam A Abduh, Belal A Al-Fuhaidi, and Fahd A Alqasemi. «Authentication Techniques in 5G Network Slicing Security: A Survey». In: *Univ. Sci. Technol. J. Eng. Technol* 2 (2024), pp. 17–36.

[2] Ibrahim Afolabi et al. «Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions». In: *IEEE Communications Surveys & Tutorials* 20.3 (2018), pp. 2429–2453. DOI: 10.1109/COMST.2018.2815638.

[3] Shams Forruque Ahmed et al. «Toward a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities». In: *IEEE Access* 12 (2024), pp. 13125–13145.

[4] Almaha Adel Almuqren. «Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions». In: *Journal of Cyber Security and Risk Auditing* 1.1 (2025), pp. 1–11.

[5] Daifallah Alotaibi. «Survey on Network Slice Isolation in 5G Networks: Fundamental Challenges». In: *Procedia Computer Science* 182 (2021). Learning and Technology Conference 2020; Beyond 5G: Paving the way for 6G, pp. 38–45. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2021.02.006. URL: https://www.sciencedirect.com/science/article/pii/S1877050921004701.

[6] Abhik Banerjee et al. «5G enabled smart cities: A real-world evaluation and analysis of 5G using a pilot smart city application». In: *Internet of Things* 28 (2024), p. 101326.

[7] Alcardo Alex Barakabitze et al. «5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges». In: *Computer Networks* 167 (2020), p. 106984.

[8] Joakim Bergström et al. «The History of Mobile Internet: The Technology Transformation That Changed the Lives of Billions». In: *Ericsson Technology Review* 2024.2 (2024), pp. 2–8. DOI: 10.23919/ETR.2024.10759706.

[9] Martin Cave. «How disruptive is 5G?» In: *Telecommunications Policy* 42.8 (2018). The implications of 5G networks: Paving the way for mobile innovation?, pp. 653–658. ISSN: 0308-5961. DOI: https://doi.org/10.1016/j.telpol.2018.05.005. URL: https://www.sciencedirect.com/science/article/pii/S0308596118301654.

[10] Nhu-Ngoc Dao et al. «A review on new technologies in 3GPP standards for 5G access and beyond». In: *Computer Networks* 245 (2024), p. 110370.

[11] Antonio Matencio Escolar et al. «Adaptive Network Slicing in Multi-Tenant 5G IoT Networks». In: *IEEE Access* 9 (2021), pp. 14048–14069. DOI: 10.1109/ACCESS.2021.3051940.

[12] Naser Al-Falahy and Omar Y Alani. «Technologies for 5G networks: Challenges and opportunities». In: *IT Professional* 19.1 (2017), pp. 12–20.

[13] José Luiz Frauendorf and Érika Almeida de Souza. «The different architectures used in 1G, 2G, 3G, 4G, and 5G networks». In: *The architectural and technological revolution of 5G*. Springer, 2022, pp. 83–107.

[14] Shujuan Gao et al. «Security threats, requirements and recommendations on creating 5G network slicing system: A survey». In: *Electronics* 13.10 (2024), p. 1860.

[15] Saqib Hakak et al. «Autonomous vehicles in 5G and beyond: A survey». In: *Vehicular Communications* 39 (2023), p. 100551.

[16] Wafa Hamdi, Orhan Dağdeviren, and Hasan Bulut. «QoS-aware Network Slicing and Resource Management for Internet of Vehicles in 5G networks». In: *Ad Hoc Networks* (2025), p. 103976.

[17] Syed Husain, Andreas Kunz, et al. «3GPP 5G Core Network: An Overview and Future Directions.» In: *Journal of Information & Communication Convergence Engineering* 20.1 (2022).

[18] Vivek Jain et al. «L25GC: A low latency 5G core network based on high-performance NFV platforms». In: *Proceedings of the ACM SIGCOMM 2022 Conference*. 2022, pp. 143–157.

[19] Alexandros Kaloxylos. «A survey and an analysis of network slicing in 5G networks». In: *IEEE Communications Standards Magazine* 2.1 (2018), pp. 60–65.

[20] Parminder Kaur, Shivani Malhotra, and Manish Sharma. «A review of isolation techniques for 5G MIMO antennas». In: *Journal of Telecommunications and Information Technology* 3 (2024), pp. 43–50.

[21] Syed Hussain Ali Kazmi et al. «Survey on joint paradigm of 5G and SDN emerging mobile technologies: Architecture, security, challenges and research directions». In: *Wireless Personal Communications* 130.4 (2023), pp. 2753–2800.

[22] Benish Sharfeen Khan et al. «URLLC and eMBB in 5G Industrial IoT: A Survey». In: *IEEE Open Journal of the Communications Society* 3 (2022), pp. 1134–1163. DOI: 10.1109/OJCOMS.2022.3189013.

[23] Latif U Khan et al. «Network slicing: Recent advances, taxonomy, requirements, and open research challenges». In: *IEEE Access* 8 (2020), pp. 36009–36028.

[24] Günter Knieps. «Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing». In: *Telecommunications Policy* 48.10 (2024), p. 102867. ISSN: 0308-5961. DOI: https://doi.org/10.1016/j.telpol.2024.102867. URL: https://www.sciencedirect.com/science/article/pii/S0308596124001642.

[25] Rajesh Kumar, Deepak Sinwar, and Vijander Singh. «QoS aware resource allocation for coexistence mechanisms between eMBB and URLLC: Issues, challenges, and future directions in 5G». In: *Computer Communications* 213 (2024), pp. 208–235.

[26] Taous Madi et al. «NFV security survey in 5G networks: A three-dimensional threat taxonomy». In: *Computer Networks* 197 (2021), p. 108283.

[27] Silvestre Malta, Pedro Pinto, and Manuel Fernandez-Veiga. «Optimizing 5G network slicing with DRL: Balancing eMBB, URLLC, and mMTC with OMA, NOMA, and RSMA». In: *Journal of Network and Computer Applications* 234 (2025), p. 104068.

[28] Kireet Muppavaram et al. «Exploring the generations: A comparative study of mobile technology from 1G to 5G». In: *Int. J. Electron. Commun. Eng* 10.7 (2023), pp. 54–62.

[29] Matteo Nerini and David Palma. «5G Network Slicing for Wi-Fi Networks». In: *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. 2021, pp. 633–637.

[30] Ruxandra F. Olimid and Gianfranco Nencioni. «5G Network Slicing: A Security Overview». In: *IEEE Communications Standards Magazine* 4.3 (2020), pp. 60–65.

[31] Rajendra Patil et al. «5G core network control plane: Network security challenges and solution requirements». In: *Computer Communications* 229 (2025), p. 107982.

[32] Shiva Raj Pokhrel et al. «Towards Enabling Critical mMTC: A Review of URLLC Within mMTC». In: *IEEE Access* 8 (2020), pp. 131796–131813. DOI: 10.1109/ACCESS.2020.3010271.

[33] Petar Popovski et al. «5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View». In: *IEEE Access* 6 (2018), pp. 55765–55779. DOI: 10.1109/ACCESS.2018.2872781.

[34] Wajid Rafique et al. «A Survey on Beyond 5G Network Slicing for Smart Cities Applications». In: *IEEE Communications Surveys & Tutorials* (2024), pp. 1–1. DOI: 10.1109/COMST.2024.3410295.

[35] Marina Settembre. «A 5g core network challenge: Combining flexibility and security». In: *2021 AEIT International Annual Conference (AEIT)*. IEEE. 2021, pp. 1–6.

[36] Murtaza Ahmed Siddiqi, Heejung Yu, and Jingon Joung. «5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices». In: *Electronics* 8.9 (2019), p. 981.

[37] Anil Thantharate et al. «Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond». In: *IEEE Transactions on Network and Service Management* 17.4 (2020), pp. 2410–2423.

[38] Mohamed Ali Torad et al. «Creating Telco Cloud to host 5G Core with DevOps Implementation». In: *The Egyptian International Journal of Engineering Sciences and Technology* 51.3 (2025), pp. 88–103.

[39] Oleg Ulyanov, Michael Schwartzman, and Harsha Sanku. *VMware Cloud on AWS Blueprint: Design, automate, and migrate VMware workloads on AWS global infrastructure*. Packt Publishing Ltd, 2024.

[40] Shalitha Wijethilaka and Madhusanka Liyanage. «Survey on network slicing for Internet of Things realization in 5G networks». In: *IEEE Communications Surveys & Tutorials* 23.2 (2021), pp. 957–994.

[41] Shalitha Wijethilaka et al. «Blockchain-Based Secure Authentication and Authorization Framework for Robust 5G Network Slicing». In: *IEEE Transactions on Network and Service Management* 21.4 (2024), pp. 3988–4005. DOI: 10.1109/TNSM.2024.3416418.

[42] Stan Wong, Bin Han, and Hans D Schotten. «5G network slice isolation». In: *Network* 2.1 (2022), pp. 153–167.

[43] Shunliang Zhang. «An Overview of Network Slicing for 5G». In: *IEEE Wireless Communications* 26.3 (2019), pp. 111–117. DOI: 10.1109/MWC.2019.1800234.

[44] Ellie Zontou. «Unveiling the evolution of mobile networks: from 1G to 7G». In: *arXiv preprint arXiv:2310.19195* (2023).