Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(Review Article)

Check for updates

Infrastructure-as-Code for 5G RAN, Core and SBI Deployment: A comprehensive review

Omoniyi David Olufemi [1, *], Ogochukwu Friday Ikwuogu [2], Eunice Kamau [3], Adedeji Ojo Oladejo [4], Adeola Adewa [5] and Olaoluwa Oguntokun [5]

[1] J. Warren McClure School of Emerging Communication Technologies, Ohio University, Athens, Ohio, USA.
[2] Faculty of Art and Science, Department of Computer Science, University of Texas Permian Basin, Texas, USA.
[3] Faculty of Information & Technology and Communications Sciences, Tampere University, Tampere, Finland.
[4] Department of Computer Science, Maharishi International University, Fairfield, Iowa, USA.
[5] Department of Electronics and Computer Engineering, Lagos State University, Lagos, Nigeria.

Global Journal of Engineering and Technology Advances, 2024, 21(03), 144-167

Publication history: Received on 16 November 2024; revised on 22 December 2024; accepted on 24 December 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.3.0235

Abstract

The advent of 5G technology marks a significant transformation in the telecommunications landscape, promising to deliver ultra-fast data speeds, minimal latency, and widespread connectivity that supports many new services and applications, including IoT, augmented reality, and autonomous systems. However, achieving the full potential of 5G networks involves overcoming substantial infrastructure challenges. Deploying and managing 5G's intricate architecture, encompassing the Radio Access Network (RAN), Core network, and Service-Based Interfaces (SBI)—requires a shift from traditional, labor-intensive methods to more advanced, automated processes. Infrastructure-as-Code (IaC) has emerged as a game-changing methodology that addresses these needs by codifying infrastructure setup and management into programmable scripts.

This comprehensive review delves into how IaC facilitates the efficient deployment and management of 5G components, enhancing agility, consistency, and scalability. By automating resource provisioning, configuration, and updates, IaC empowers network operators to rapidly deploy infrastructure that meets the demanding requirements of 5G services. The paper discusses how IaC enables seamless integration and scaling of network functions, improves operational efficiency through reduced human error, and supports consistent infrastructure management across distributed environments. Key tools such as Terraform, Ansible, and Kubernetes are explored, showcasing their applications in orchestrating various layers of the 5G network, from RAN deployment to core network orchestration and SBI configurations.

Despite its advantages, adopting IaC in 5G deployment comes with its challenges. These include managing the complexities inherent in multi-vendor environments, ensuring robust security for automated provisioning scripts, and maintaining compliance with regional regulatory standards. The paper explores these obstacles in-depth, offering insights into best practices and potential solutions to navigate these hurdles.

This review highlights emerging trends and research opportunities, such as the potential for zero-touch automation, which leverages IaC for autonomous network operations with minimal human intervention. It also discusses the role of artificial intelligence (AI) and machine learning (ML) in predictive resource management and automated fault detection, proposing a future where AI-enhanced IaC can revolutionize the deployment and operation of 5G networks. By examining these elements, the review aims to provide a holistic view of the current state and future trajectory of IaC in 5G RAN, Core, and SBI deployment, setting the stage for ongoing innovation and development in the field.

* Corresponding author: Omoniyi David Olufemi

Keywords: Infrastructure-as-Code (IaC); Service-Based Interface (SBI); Zero-Touch Automation; CI/CD; Network Slicing; DevOps; AI

1. Introduction

The emergence of 5G technologies represents a pivotal evolution in the field of telecommunications, bringing unprecedented speed, connectivity, and potential for innovation across industries. Unlike previous generations of wireless technology, 5G is designed to support a wide range of complex use cases, from enhanced mobile broadband and massive machine-type communications (mMTC) to ultra-reliable low-latency communications (URLLC) [1]. These diverse applications introduce sophisticated performance requirements that demand a robust, scalable, and agile infrastructure that adapts to varying network conditions and user demands. The deployment of 5G infrastructure, however, poses significant challenges that cannot be adequately addressed using traditional methods of infrastructure management, which rely heavily on manual configuration and siloed processes.

Infrastructure-as-Code (IaC) has emerged as a transformative methodology that meets these modern needs by automating the provisioning, configuring, and managing of infrastructure through machine-readable scripts. IaC allows network operators to define and deploy infrastructure programmatically, enabling rapid, repeatable, and error-free configuration of network components [2]. This is particularly valuable for 5G deployment, where the architecture is more complex than ever, involving distributed components, network slicing, and service-based interactions. The ability to quickly scale and modify infrastructure through code is essential for meeting the high demands of 5G services, which include real-time data processing for autonomous vehicles, remote healthcare, smart cities, and industrial automation.

This review focuses on the critical role that IaC plays in deploying and managing key 5G network components: the Radio Access Network (RAN), the Core network, and the Service-Based Interfaces (SBI). The RAN forms the link between end-user devices and the broader network, necessitating highly scalable and adaptive infrastructure to manage varying user densities and geographic coverage. The Core network is central to data processing and management, incorporating advanced functions such as network slicing and network function virtualization (NFV) to support different quality-of-service (QoS) levels [3]. The SBI, on the other hand, facilitates communication between network functions using web-based protocols, ensuring that the entire ecosystem operates cohesively.

IaC provides substantial advantages by enabling network operators to automate complex workflows, scale infrastructure on demand, and maintain consistency across network deployments. IaC reduces human intervention and the potential for configuration drift through automated configuration and management, thus enhancing reliability and operational efficiency. It also supports continuous integration and deployment (CI/CD) pipelines, crucial for maintaining an agile development and deployment cycle that keeps pace with rapidly evolving 5G technologies and services.

Despite its apparent benefits, adopting IaC in 5G deployment is challenging. The inherent complexity of multi-vendor environments, where components come from various suppliers with distinct standards and interfaces, can complicate IaC implementation. Moreover, while automation brings significant efficiency, it also introduces potential security risks, as vulnerabilities in IaC scripts or repositories could expose critical network infrastructure to threats. Ensuring robust security measures and stringent access controls for IaC configurations is essential to mitigate these risks. Additionally, 5G deployments must adhere to varying regulatory and compliance requirements across different regions, requiring IaC scripts to be flexible enough to adapt to these conditions without compromising performance or security.

This comprehensive review aims to explore how IaC is utilized in deploying 5G RAN, Core, and SBI components, examining its benefits, such as enhanced scalability, operational efficiency, and consistency, as well as the challenges of its implementation. Furthermore, this paper will discuss the current tools and frameworks used in IaC, including Terraform, Ansible, and Kubernetes, and provide insights into emerging trends and future research opportunities, such as the integration of artificial intelligence (AI) and machine learning (ML) for predictive and autonomous infrastructure management. By presenting a detailed analysis of these aspects, this review offers valuable knowledge for network operators, engineers, and researchers involved in the evolution and optimization of 5G infrastructure deployment.

2. Infrastructure-as-Code: Definition and Relevance to 5G Deployment

Infrastructure-as-Code (IaC) is a modern paradigm that shifts the management and provisioning of computing infrastructure from manual processes to automated, code-driven methodologies. At its Core, IaC involves using declarative or imperative code to define, provision, configure, and update infrastructure components [4]. This approach aligns closely with the principles of **DevOps**, which emphasize continuous integration, continuous delivery (CI/CD), collaboration between development and operations teams, and a culture of automation to enhance agility and efficiency.

In the context of 5G deployment, IaC is indispensable due to the intricate and dynamic nature of 5G architecture. Unlike its predecessors, 5G technology is designed to support a wide array of applications, from enhanced mobile broadband (eMBB) and ultra-reliable low-latency communications (URLLC) to massive machine-type communications (mMTC) [5]. These capabilities demand infrastructure that is highly scalable, reliable, and capable of adapting rapidly to changing network conditions and user demands. IaC provides a means to achieve these requirements by treating infrastructure as a programmable entity, enabling network operators to define infrastructure through machine-readable scripts that automate complex tasks such as provisioning, scaling, and lifecycle management.

2.1. Key Concepts of IaC Relevant to 5G Deployment

2.1.1. Declarative vs. Imperative Approaches

- **Declarative IaC** tools, such as Terraform and Kubernetes, focus on defining the desired state of the infrastructure, allowing the system to determine how to reach that state. This is particularly beneficial for 5G because it simplifies the management of complex multi-layered infrastructure components, such as Radio Access Networks (RAN), Core Networks, and Service-Based Interfaces (SBI) [6].
- **Imperative IaC** tools, like Ansible, define the steps to achieve the desired state, providing greater control over how changes are executed. This method is often used for fine-tuning and specific tasks within a 5G deployment, such as configuring network functions virtualization (NFV) or updating network slices [7].
- **Version Control and Consistency**: One significant advantage of IaC is that infrastructure configurations are stored as code in version control systems like Git. This allows consistent infrastructure replication across multiple environments, ensuring uniformity from development to production. In 5G deployment, where distributed units (DUs), centralized units (CUs), and edge computing nodes must maintain coherent configurations across different sites, version-controlled IaC scripts prevent configuration drift and maintain operational consistency.
- **Scalability and Automation**: **5G networks** inherently require rapid scalability to manage varying loads, especially in high-user density scenarios or applications that demand real-time processing. IaC allows network operators to automate the scaling of resources, such as provisioning additional RAN nodes or deploying more virtual network functions (VNFs) in response to increased demand. This automation extends to load balancing, traffic routing, and orchestration of containers and microservices, which are pivotal for the high-performance requirements of 5G networks.
- **CI/CD Integration and DevOps Alignment**: IaC integrates seamlessly with CI/CD pipelines, enabling automated testing, validation, and deployment of infrastructure changes. This is critical for 5G networks that need to be updated regularly to support new features, patches, or service expansions. IaC within DevOps practices can push changes more frequently and reliably without the risk of human error. This aligns with the need for continuous deployment and monitoring in the 5G ecosystem to maintain service quality and adapt to rapid technological advancements.
- **Reproducibility and Idempotency**: A core characteristic of IaC is idempotency, which ensures that applying the same configuration script multiple times results in the same infrastructure state. This feature is significant in 5G, where reproducibility across multiple distributed data centers or edge nodes is essential for maintaining service consistency and minimizing latency. Idempotency reduces the risk of discrepancies that could affect the quality of service (QoS), ensuring that each part of the network performs predictably, from core nodes to edge computing resources.
- **Integration with Orchestration Tools**: In 5G, the management of containerized services and microservices architectures is facilitated by tools like Kubernetes and Helm charts, which function as extensions of IaC. These tools provide the orchestration needed for deploying and managing complex services across cloud-native environments. This is crucial for the core network components that utilize container network functions (CNFs), enabling 5G to deliver enhanced flexibility and service modularity.

2.1.2. Relevance of IaC to 5G Deployment

The relevance of IaC in 5G deployment is underscored by its ability to manage and automate the lifecycle of highly complex and distributed network architectures. Key areas where IaC plays a vital role include:

- **Automated Deployment of RAN and Core Infrastructure**: IaC enables the rapid deployment of RAN components, such as DUs and CUs, as well as core network functions like Access and Mobility Management

Function (AMF) and User Plane Function (UPF) [8]. This automation is crucial for meeting the deployment timelines and scaling requirements inherent to 5G rollouts.
- **Service-Based Architecture (SBA) Configuration**: The SBI in 5G allows communication between network functions using modern web protocols. IaC facilitates the setup of APIs and the deployment of microservices that form the backbone of SBA, ensuring seamless interoperability and service delivery [9].
- **Edge Computing Integration**: The low-latency applications in 5G, such as augmented reality (AR) and autonomous driving, rely on edge computing. IaC streamlines the deployment and management of edge nodes, enabling them to be provisioned automatically and maintained consistently.
- **Dynamic Resource Management**: IaC's inherent flexibility allows for the real-time allocation of resources across the network, adapting to traffic patterns and optimizing bandwidth utilization. This is particularly important for maintaining the high QoS needed for 5G applications that require stringent latency and bandwidth guarantees.
- **Support for Network Slicing**: IaC provides the framework to implement and manage network slicing, which segments the physical infrastructure into multiple virtual networks tailored for specific use cases [10]. This capability ensures that IoT devices, enterprise applications, and critical services receive the appropriate resource allocation and priority.

IaC is a cornerstone in deploying 5G infrastructure, serving as an essential tool to automate, scale, and manage complex network components. Its integration with DevOps practices, support for continuous delivery, and ability to maintain consistency across distributed environments make it a critical enabler for the agile and efficient operation of 5G networks. As 5G technology evolves, using IaC with advanced orchestration and automation tools will pave the way for even more sophisticated and reliable network architecture, ultimately driving the next phase of telecommunications innovation.

3. 5G Network Architecture Overview

The 5G network architecture is designed to meet the diverse demands of modern telecommunications, supporting a range of services from ultra-high-speed Internet to mission-critical applications requiring near-zero latency. This modular and layered architecture comprises the Radio Access Network (RAN), Core Network, and Service-Based Interface (SBI), each with distinct components, nodes, and microservices contributing to its operation. This section explains these components and how they function to deliver seamless, efficient communication.

3.1. Radio Access Network (RAN)

The **5G Radio Access Network (RAN)** is responsible for connecting user devices to the core network and handling the transmission and reception of data over radio frequencies. The 5G RAN is distinguished by its split architecture, which optimizes performance and scalability using Centralized Units (CUs) and Distributed Units (DUs).

3.1.1. Overview of the Key Nodes and Interfaces in 5G RAN:

- **Distributed Unit (DU)**: The DU is responsible for managing lower-layer protocols, including the Physical (PHY) layer and parts of the Medium Access Control (MAC) layer [11]. DUs are located closer to end-user devices, typically at cell sites or on towers, and handle real-time processing tasks such as beamforming and signal modulation. By distributing processing power to DUs, 5G RAN can reduce latency and improve local data handling, crucial for applications like autonomous vehicles and smart city sensors.
- **Centralized Unit (CU)**: The CU manages higher-layer protocols, such as Radio Resource Control (RRC) and Packet Data Convergence Protocol (PDCP), and oversees broader, non-time-critical functions [12]. CUs are usually located in data centers and manage resources across multiple DUs, facilitating network optimization and load balancing.

3.1.2. Interfaces

- **F1 Interface**: This interface connects the CU and DU, enabling communication and coordination between these units. It ensures the seamless transfer of data packets and control signals, balancing the workload between centralized and distributed processing.
- **Xn Interface**: This interface facilitates communication between different CUs to support seamless **handover** processes when users move between cells or regions. It is vital for maintaining connection continuity and optimal data transfer.
- **Microservices in 5G RAN**: 5G RAN is increasingly adopting microservices architecture to support scalability and flexibility. This means that network functions within the CU and DU are broken down into minor,

containerized services that can be deployed and managed independently. Microservices enable rapid scaling and efficient resource management, which is essential for addressing high user densities and variable traffic loads [13].

3.2. Core Network

The **5G Core Network** (5GC) is the backbone of 5G, managing data flow, user authentication, policy enforcement, and network slicing. The 5GC uses a service-based architecture (SBA) that leverages cloud-native technologies, enabling greater flexibility and modularity.

3.2.1. Key Nodes in the 5G Core Network:

- **Access and Mobility Management Function (AMF)**: This function handles user equipment (UE) registration, connection, and mobility management. The AMF acts as UE's first point of contact and coordinates with other network functions to ensure user connectivity and service continuity.
- **Session Management Function (SMF)**: This function manages session establishment, modification, and termination for data connections. It plays a crucial role in assigning IP addresses and ensuring efficient Quality of Service (QoS) management.
- **User Plane Function (UPF)**: This function manages data packet routing and forwarding between the RAN and external data networks. It enables low-latency data transmission and supports network slicing, allowing the Core to handle different data streams with varying service-level agreements.
- **Network Slice Selection Function (NSSF)**: This node allocates and manages network slices, which are isolated segments of the network tailored for specific services, such as IoT devices or high-speed data applications. This node ensures that each service receives the appropriate resources and bandwidth.
- **Policy Control Function (PCF)**: Central to policy management, PCF oversees rules that define how network resources are used, impacting bandwidth allocation, prioritization, and data handling.
- **Unified Data Management (UDM)** and **Unified Data Repository (UDR)**: Manage and store subscriber information and service data, enabling authentication and authorization processes.

3.2.2. Overview of the major Interfaces in the 5G Core Network:

- **N2 Interface**: This interface connects the AMF and RAN to manage control-plane functions, facilitating the exchange of signaling information necessary for mobility and session management.
- **N3 Interface**: This interface connects the RAN to the UPF and handles user-plane data traffic between the access network and external data networks.
- **N6 Interface**: This interface connects the UPF to data networks or services outside the 5G system, playing a critical role in interfacing with the Internet and enterprise networks.
- **Microservices in the Core Network**: The SBA of the 5G Core is underpinned by a microservices architecture, wherein each network function is a microservice that interacts with others through APIs. This modular approach allows for independent scaling, updates, and service management, making the Core more adaptable and resilient to changes in network demand. Containerized platforms like Docker and orchestration tools like Kubernetes are commonly used to manage these microservices, ensuring efficient resource allocation and high availability [14].

3.3. Service-Based Interface (SBI)

The **Service-Based Interface (SBI)** is a defining feature of the 5G Core's architecture. It facilitates communication between network functions through standardized web-based protocols, typically HTTP/2 and RESTful APIs. This approach contrasts with previous network generations' tightly coupled, proprietary interfaces and introduces greater flexibility and interoperability.

3.3.1. Core Components of SBI

- **Network Functions as Services**: In a service-based architecture, network functions such as AMF, SMF, and UPF communicate using the SBI. Each function can request services from another, promoting a modular and scalable network design.
- **API Gateways**: API gateways manage and secure interactions between network functions. They handle tasks such as authentication, rate limiting, and load balancing, ensuring that SBI communications remain secure and efficient.

- **Service Registries**: Act as directories for available network functions and services, allowing functions to dynamically discover and interact with one another. This feature supports load distribution and enhances network resiliency by directing requests to the appropriate service instance.
- **Microservices in SBI**: SBI facilitates a microservices approach by decoupling network functions and enabling them to be deployed as standalone services. Each microservice is responsible for a specific task, such as user authentication or data routing, and can be scaled independently to meet traffic demands [15]. This model aligns with cloud-native principles, supporting rapid deployment, containerization, and orchestration through tools like Kubernetes and Helm charts.

3.3.2. What are the Interfaces and Communication Protocols?

- **HTTP/2**: Provides enhanced performance through features like multiplexing, header compression, and flow control, which improve the efficiency of data exchange between network functions.
- **RESTful APIs**: Facilitate standardized communication and service requests, enabling seamless integration and interaction between different microservices.
- **gRPC**: An emerging protocol for high-performance communication between microservices, offering better speed and efficiency than traditional RESTful APIs, making it suitable for real-time 5G applications.

The 5G network architecture, comprising the RAN, Core Network, and SBI, relies heavily on cloud-native technologies and modular structures to meet modern connectivity demands. Each component—DUs and CUs in the RAN, key nodes in the Core Network, and service interactions via the SBI—uses microservices to achieve flexibility, scalability, and high availability [16]. Infrastructure-as-Code (IaC), containerization, and orchestration platforms support the dynamic and agile nature of 5G, laying the groundwork for robust, adaptable, and efficient telecommunication services.

4. IaC Implementation Across 5G Components

Deploying **Infrastructure-as-Code (IaC)** across 5G network components is crucial for achieving scalable, consistent, and efficient infrastructure management. This chapter explores how IaC is applied in various segments of the 5G architecture, including the **Radio Access Network (RAN)**, **Core Network**, and **Service-Based Interface (SBI)**. Each section delves into the specifics of how IaC automates provisioning, scaling, and management, contributing to the overall agility and reliability of 5G services.

4.1. IaC in RAN Deployment

The **Radio Access Network (RAN)** is the frontline of 5G, connecting user equipment (UE) to the broader network. The 5G RAN is designed with a disaggregated architecture consisting of Distributed Units (DUs) and Centralized Units (CUs). This segmentation allows for flexibility and optimized resource allocation, essential for meeting the diverse demands of 5G applications. Implementing IaC in RAN deployment offers significant advantages by automating the provisioning and management of DUs and CUs.

4.1.1. Automation of DUs and CUs

- **Distributed Units (DUs)**: DUs handle the **Physical (PHY)** and **Medium Access Control (MAC)** layers and perform real-time signal processing. By using IaC, operators can automate the deployment of DUs across multiple cell sites [17]. Scripts can define network configurations, allocate IP addresses, manage beamforming, and configure low-latency processing functions, ensuring rapid and consistent deployment.
- **Centralized Units (CUs)**: CUs manage the Radio Resource Control (RRC) and Packet Data Convergence Protocol (PDCP) layers, centralizing non-real-time processing tasks. IaC scripts automate the setup of CUs in data centers where high computing power is available. These scripts configure protocols, apply security settings, and manage connections to DUs via the F1 interface.
- **Dynamic Resource Scaling**: IaC is vital in enabling dynamic scaling of RAN components. By integrating IaC scripts with orchestration tools such as Kubernetes and Terraform, network operators can provision additional DUs and CUs in response to network traffic changes. For example, IaC scripts can automatically deploy additional DUs during peak hours or special events to support increased user density. Conversely, resources can be scaled down during off-peak periods to optimize energy consumption and operational costs.
- **Configuration Management and Version Control**: Version-controlled IaC scripts ensure that all DUs and CUs are configured uniformly, reducing the risk of configuration drift. This consistency is particularly crucial for maintaining the quality of service (QoS) across a wide geographic area. Using tools like Ansible or Puppet, operators can simultaneously push configuration updates across multiple units, ensuring that new features or patches are deployed without discrepancies [18].

4.2. IaC in Core Network Deployment

The **5G Core Network (5GC)** is the central hub for managing data routing, user mobility, policy control, and network slicing. The 5GC employs a Service-Based Architecture (SBA) that leverages cloud-native technologies to deliver high modularity and flexibility. Implementing IaC in the deployment of the core network facilitates the efficient management of network functions and supports the adoption of Network Functions Virtualization (NFV).

4.2.1. Automating Network Functions with IaC:

- **Access and Mobility Management Function (AMF)**: IaC scripts can define and deploy AMF instances, automating configurations related to user registration, mobility management, and session handling. By coding these processes, operators can quickly scale AMFs to handle user surges without manual intervention.
- **Session Management Function (SMF)** and User Plane Function (UPF): SMF manages data sessions, while UPF handles data packet forwarding. IaC allows these network functions to be provisioned, configured, and updated consistently and repeatably, supporting real-time traffic demands and reducing latency.
- **Network Slice Configuration**: IaC's ability to automate network slicing is particularly valuable for 5G. Scripts can define slice-specific attributes, such as bandwidth allocation, priority levels, and QoS settings, ensuring that each slice meets the needs of specific applications, whether massive IoT or ultra-low-latency communications [19].
- **NFV and Containerization**: IaC enables the deployment of NFV, where network functions are decoupled from proprietary hardware and run as software instances on virtual machines (VMs) or containers. Using **Docker** and **Kubernetes**, operators can deploy containerized network functions as microservices. For example, IaC scripts can create and manage Kubernetes deployments that house containerized versions of AMF, SMF, and UPF, providing a scalable and flexible framework for core network operations.
- **Continuous Integration and Deployment (CI/CD)**: Integrating IaC with CI/CD pipelines ensures that updates and patches to core network functions are automated and thoroughly tested before deployment. This practice minimizes downtime and reduces the risk of human error. By using tools like Jenkins or GitLab CI/CD, IaC scripts can be automatically applied after passing validation checks, promoting a seamless update process across the core network.

4.3. IaC in SBI Configuration and Management

The **Service-Based Interface (SBI)** is an essential element of the 5G Core Network's service-based architecture. It enables communication between network functions through standardized web-based protocols, such as HTTP/2 and RESTful APIs. IaC is critical in managing and configuring these interactions to ensure efficient and scalable service delivery.

- **Dynamic API Configuration**: IaC can automate the deployment and configuration of APIs that form the backbone of SBI. Through IaC scripts, network operators can specify the endpoints, request methods, and security protocols required for network function interactions. This automation ensures that APIs are configured consistently across multiple network functions, reducing the risk of misconfigurations that could affect communication or security.
- **Service Discovery and Load Balancing**: SBI relies on service discovery mechanisms to allow network functions to dynamically locate and interact with each other. IaC facilitates the deployment of service registries, such as Consul or etcd, which maintain a directory of available services and their statuses. IaC scripts can also define load balancing rules and failover protocols to distribute traffic evenly and ensure service reliability.
- **Security and Compliance**: With IaC, security policies for SBI interactions can be codified and enforced uniformly. IaC scripts can include the deployment of API gateways that handle authentication, authorization, and rate limiting for API traffic. This ensures that sensitive operations, such as user authentication managed by the AMF, are protected against unauthorized access and attacks. By integrating IaC with security tools like HashiCorp Vault, secrets management and secure access to API credentials are automated, reducing the risk of exposure [20].
- **Containerized Microservices Management**: The use of containerized microservices in the 5G Core Network aligns with the modular nature of SBI. IaC enables operators to deploy and orchestrate these microservices, ensuring they scale based on network conditions. For instance, IaC scripts can be used to scale out microservices, handle policy control when data usage peaks, maintain QoS and prevent service degradation.
- **Observability and Monitoring**: IaC supports the deployment of observability tools such as Prometheus and Grafana, which monitor the health and performance of SBI communications. Network functions are instrumented for logging and monitoring through automated deployment scripts, allowing operators to receive

real-time data on API response times, error rates, and service availability [21]. This data-driven approach helps diagnose issues proactively and maintain seamless service continuity.

IaC significantly enhances the deployment and management of 5G RAN, Core, and SBI components by automating the provisioning, scaling, and updating processes. For the RAN, IaC ensures that DUs and CUs are deployed quickly and consistently, while in the core network, it streamlines the management of essential functions like AMF, SMF, and UPF, supporting NFV and containerized microservices. In the SBI, IaC automates API configurations and enforces security measures, enabling dynamic and secure interactions among network functions. This comprehensive approach improves the agility and scalability of 5G networks and supports continuous delivery and real-time adaptability, which are critical for modern telecommunications.

5. Benefits of IaC in 5G RAN, Core, and SBI Deployment

Deploying Infrastructure-as-Code (IaC) in 5G networks provides transformative advantages, addressing modern telecommunications's complexities and dynamic demands. Implementing IaC across 5G Radio Access Network (RAN), Core Networks, and Service-Based Interface (SBI) enhances operational capabilities and supports the scalability, efficiency, and reliability required for advanced 5G services. This chapter explores these benefits in detail, highlighting how IaC optimizes 5G network infrastructure deployment and management.

5.1. Scalability and Flexibility

Scalability is a crucial requirement for 5G networks due to the fluctuating nature of user demand, application-specific requirements, and the need to accommodate diverse traffic loads across different regions and times. IaC offers unmatched scalability and flexibility through its ability to automate the provisioning and de-provisioning of infrastructure components.

5.1.1. Scalability in 5G RAN:

5G scalability can be seen from two key areas:

- **Automated Deployment of DUs and CUs**: IaC allows rapidly deploying of Distributed Units (DUs) and Centralized Units (CUs) based on real-time network needs. For example, IaC scripts can automatically scale up the number of active DUs during high-traffic events or peak hours to handle increased data flow [21]. This adaptability ensures that user experience remains seamless, without the risk of network congestion.
- **Load Management**: By integrating with tools such as Kubernetes and Terraform, IaC can deploy containerized network functions that automatically scale horizontally or vertically. This capability supports elastic load management and ensures that network resources are utilized efficiently, minimizing latency and optimizing data throughput.

5.1.2. Flexibility in 5G Core and SBI:

- **Dynamic Core Network Functions**: IaC facilitates the flexible scaling of core network functions such as the User Plane Function (UPF) and Session Management Function (SMF). This is critical for applications that experience rapid changes in user demand, such as streaming services and interactive gaming. The ability to scale core network functions based on traffic ensures that the Core can meet service-level agreements (SLAs) for different types of applications [22].
- **SBI Communication Scaling**: The Service-Based Interface (SBI) benefits from IaC by dynamically configuring and scaling APIs that manage interactions between network functions. IaC scripts can deploy additional API gateways or microservices instances when service demands increase, maintaining low response times and efficient data handling.

5.2. Operational Cost Reduction

One of the most significant advantages of implementing IaC is reducing operational expenses through automation. Traditional infrastructure management methods often require manual configuration and significant human resources for maintenance and updates, leading to high operational costs. IaC mitigates these costs through the following mechanisms:

5.2.1. Automation of Routine Tasks

- **Reduced Manual Labor**: IaC automates repetitive and complex tasks such as provisioning DUs, configuring network slices, or deploying security patches. This reduces the need for extensive human involvement, freeing up skilled personnel to focus on higher-value tasks such as strategic network planning and optimization.
- **Automated Error Detection and Remediation**: IaC scripts can include built-in checks that automatically identify and resolve configuration errors. This self-healing capability minimizes downtime and reduces the costs associated with manual troubleshooting and recovery efforts.

5.2.2. Efficient Resource Utilization

- **On-Demand Resource Management**: IaC enables resources to be scaled up or down as needed, avoiding over-provisioning, which can lead to unnecessary expenditure. During periods of low traffic, IaC scripts can automatically decommission or scale down resources, resulting in cost savings.
- **Optimal Deployment Strategy**: By leveraging IaC, network operators can deploy infrastructure efficiently in cloud or hybrid environments, using the most cost-effective combination of on-premises and cloud resources to achieve operational goals.

5.3. Consistency and Reliability

Consistency across network components is essential to ensure smooth operation and minimize the risk of performance degradation due to configuration drift or human error. IaC contributes significantly to the reliability and uniformity of 5G network deployments through the following:

5.3.1. Uniform Configurations Across Deployments

- **Version Control**: IaC scripts are stored in version-controlled repositories such as **Git**, allowing network operators to track changes, manage revisions, and revert to previous configurations if necessary. This ensures that all infrastructure deployments, from RAN nodes to core functions and SBI interactions, are consistent across different environments [23].
- **Golden Configurations**: IaC supports using standardized, or "golden," configurations that define optimal settings for infrastructure components. These golden configurations are deployed consistently, preventing inconsistencies leading to security vulnerabilities or service disruptions.

5.3.2. Reduced Configuration Drift

- **Automated State Management**: IaC tools such as **Ansible** and **Terraform** maintain the desired state of the infrastructure. If deviations occur, IaC scripts automatically correct them, ensuring network components remain aligned with predefined configurations. This feature is significant in 5G networks that span vast geographical areas with numerous interconnected nodes and services [24].

5.3.3. Reliability in SBI Communications

- **Consistent API Configuration**: IaC ensures that APIs facilitating communication between core network functions are configured uniformly. This prevents communication issues arising from misconfigurations and enhances the reliability of service-based interactions.
- **Policy Enforcement**: By codifying security policies within IaC scripts, operators can enforce consistent access controls and authentication protocols across all network layers, reducing the likelihood of unauthorized access or data breaches.

5.4. Speed and Deployment Efficiency

Deploying infrastructure rapidly is essential in the fast-paced telecommunications industry, where new services and updates must be rolled out quickly to remain competitive. IaC contributes to deployment speed and efficiency in several ways:

5.4.1. Rapid Deployment of 5G Components

- **Automated Provisioning**: IaC scripts enable the automated deployment of DUs, CUs, and core network functions within minutes, a process that would otherwise take days or weeks using manual methods. This is particularly beneficial for urgent deployments, such as those needed to support special events or rapid service expansions.

- **Predefined Templates**: IaC allows operators to use predefined templates for different types of deployments. These templates ensure that deployments follow best practices and can be launched quickly without needing custom development each time.

5.4.2. Integration with CI/CD Pipelines

- **Continuous Integration/Continuous Deployment (CI/CD)**: IaC integrates seamlessly with CI/CD pipelines, enabling automated testing, validation, and deployment of infrastructure changes. Tools like Jenkins, GitLab CI/CD, and Azure DevOps facilitate this integration, ensuring that new updates are automatically tested and applied to production environments without manual intervention. This approach minimizes the risk of downtime and enhances the speed at which new features or patches are rolled out.
- **Automated Rollbacks**: If an update fails or introduces issues, IaC scripts can include rollback mechanisms that revert the infrastructure to its previous stable state [25]. This capability ensures minimal disruption to services, maintaining high availability and user satisfaction.

5.4.3. Scalable Edge Deployments

- **Deployment of Edge Nodes**: With 5G applications requiring low latency, IaC enables rapid deployment of edge computing nodes to process data closer to end-users. This quick deployment supports services like augmented reality (AR) and IoT applications, which demand high processing speeds and minimal delays.
- **Microservices Orchestration**: The microservices architecture in 5G, facilitated by container orchestration tools like Kubernetes, allows for the fast and efficient scaling of services at the edge and Core. IaC plays a critical role in deploying and managing these containers, ensuring that microservices are configured and operational quickly.

The implementation of IaC in 5G RAN, Core, and SBI deployment offers unparalleled benefits. It enables scalable and flexible infrastructure, reduces operational costs, ensures consistency and reliability, and accelerates deployment speeds. By integrating IaC with advanced tools and frameworks, network operators can achieve seamless management of 5G networks, support dynamic service demands, and maintain a competitive edge in the rapidly evolving telecommunications landscape [26].

6. Challenges in Implementing IaC for 5G

While Infrastructure-as-Code (IaC) offers numerous advantages for deploying and managing 5G networks, its implementation comes with specific challenges that must be addressed to ensure seamless and secure operations. These challenges are particularly pronounced due to the complex, distributed, and dynamic nature of 5G architectures. This chapter delves into the primary obstacles faced when implementing IaC for 5G deployment, focusing on multi-vendor environments, security risks, network slicing, orchestration, and regulatory compliance.

6.1. Complexity in Multi-Vendor Environments

Multi-vendor environments are a common characteristic of 5G deployments, where different parts of the network—such as Radio Access Network (RAN), Core Network, and Service-Based Interface (SBI) components—are sourced from various vendors [27]. Each vendor often employs proprietary configurations, interfaces, and protocols, creating significant challenges for standardization and compatibility when using IaC.

6.1.1. Interoperability Issues

- **Heterogeneous Infrastructure**: Using different hardware and software from multiple vendors leads to varying management interfaces, configurations, and requirements. IaC scripts must be flexible and customizable enough to accommodate these differences while maintaining a coherent overall deployment strategy.
- **Vendor-Specific APIs**: Some vendors provide their own APIs or proprietary tools for managing network functions, which may align differently with open-source or widely used IaC tools like Terraform or Ansible [28]. This discrepancy requires additional custom coding and adaptations in IaC scripts to ensure smooth operation across diverse platforms.

6.1.2. Standardization Challenges

- **Lack of Unified Standards**: The absence of universally accepted standards for defining and deploying network functions complicates using IaC in multi-vendor environments. Network operators may need help in integrating IaC practices with specific vendor technologies, leading to potential delays and increased costs.
- **Increased Complexity in Maintenance**: Maintaining consistency and coherence across IaC configurations in a multi-vendor environment requires continuous updates and modifications to accommodate vendor-specific changes or updates, adding complexity to long-term infrastructure management.

6.2. Security Risks

Security is critical in any automated infrastructure deployment, and IaC is no exception. If not properly secured, IaC scripts can introduce vulnerabilities that may be exploited, posing significant risks to 5G networks.

6.2.1. Potential Vulnerabilities in IaC

- **Exposure of Sensitive Data**: IaC scripts often include configuration details such as access credentials, API keys, and network configurations. If these scripts are not securely stored or encrypted, they could expose sensitive data, making the network vulnerable to unauthorized access and attacks [29].
- **Code Injection and Tampering**: IaC code repositories that are not adequately protected may be susceptible to tampering or malicious code injection. This can lead to unauthorized changes in infrastructure configurations, potentially resulting in service disruptions or compromised network security.

6.2.2. Best Practices for Mitigating Security Risks

- **Secrets Management**: Utilizing tools like HashiCorp Vault or AWS Secrets Manager can help securely store and access sensitive information without embedding it directly in IaC scripts.
- **Access Control and Permissions**: Implementing strict access controls and role-based permissions ensures that only authorized personnel can modify or execute IaC scripts. This reduces the risk of insider threats and accidental misconfigurations.
- **Regular Code Audits and Reviews**: Regular security reviews and audits of IaC scripts help identify and address vulnerabilities before they can be exploited. Automated tools such as Snyk and Checkov can be used to scan IaC code for potential security issues [30].

6.3. Network Slicing and Orchestration

Network slicing is one of the defining features of 5G, allowing operators to create multiple virtual networks within a single physical network infrastructure. Each network slice can be configured to meet specific service requirements, such as high bandwidth for streaming or low latency for IoT applications. However, managing network slices with IaC poses significant challenges due to the complexity involved.

6.3.1. Challenges in Network Slicing:

- **Complex Orchestration Requirements**: Orchestrating multiple network slices with different configurations, QoS requirements, and performance metrics requires sophisticated IaC scripts that can handle the dynamic nature of slicing. These scripts must coordinate the deployment and management of various network functions across RAN, Core, and SBI, ensuring each slice operates independently while sharing physical resources [31].
- **Real-Time Adjustments**: 5G networks often need to adjust slice parameters in real time to respond to changing traffic conditions and user demands. Writing IaC scripts that can support such real-time modifications without interrupting existing services adds complexity to their design and implementation.

6.3.2. Integration with Orchestration Platforms

- **Kubernetes and Containers**: IaC can manage containerized microservices for network slices, but integrating IaC with platforms like Kubernetes and orchestration tools like Helm or OpenShift can be intricate. These platforms must be configured to deploy and monitor network slices, scale resources dynamically, and maintain service continuity.
- **Service Assurance**: Ensuring that each network slice meets its SLA requires comprehensive monitoring and assurance mechanisms, which must be integrated into IaC scripts. This includes setting up observability tools like Prometheus and Grafana to track metrics like latency, throughput, and error rates for each slice.
-

6.4. Compliance with Regulatory Standards

5G networks must comply with various regulatory and legal requirements that differ from region to region. Implementing IaC in a way that adheres to these regulations poses challenges, as it requires a flexible yet standardized approach to script development and execution.

6.4.1. Regulatory Challenges

- **Data Sovereignty**: Regulations often mandate that data be stored and processed within specific geographic boundaries. IaC scripts must be adapted to deploy infrastructure compliant with these data localization laws, which may involve defining location-specific parameters and using region-specific cloud providers.
- **Privacy and Security Regulations**: Ensuring that IaC deployments meet requirements such as the General Data Protection Regulation (GDPR) or other local data privacy laws can be complex. Scripts must incorporate measures to secure user data and manage access logs in compliance with these standards.

6.4.2. Adapting IaC Scripts for Compliance

- **Custom Templates and Modules**: To adhere to various regulatory requirements, IaC templates and modules can be customized for different regions. This enables network operators to maintain compliance without having to rewrite scripts for each jurisdiction.
- **Policy as Code**: Implementing policy as code frameworks, such as OPA (Open Policy Agent), allows network operators to define and enforce compliance policies programmatically within IaC scripts. This ensures that any infrastructure changes adhere to predefined regulatory and security guidelines.

6.4.3. Documentation and Auditing

- **Automated Documentation**: IaC scripts should include automated documentation capabilities to generate logs and reports of infrastructure changes. These logs can be invaluable for demonstrating compliance during regulatory audits.
- **Auditable Workflows**: Integrating IaC with compliance tools ensures that all infrastructure changes can be tracked and audited, making identifying and resolving non-compliance issues easier.

Implementing IaC for 5G deployment introduces significant benefits, but it has challenges. The complexity of multi-vendor environments, potential security risks, sophisticated network slicing and orchestration needs, and adherence to regulatory standards are all areas that require careful attention [32]. By recognizing and addressing these challenges, network operators can optimize their IaC strategies and leverage their capabilities to build a robust, scalable, and secure 5G infrastructure.

7. Current IaC Tools and Technologies

The deployment of Infrastructure-as-Code (IaC) in 5G networks relies on various tools and platforms that cater to different aspects of infrastructure provisioning, configuration management, and orchestration. Each tool has its strengths and is chosen based on the specific requirements of the 5G component being managed, whether it be the Radio Access Network (RAN), Core Network, or Service-Based Interface (SBI) [33]. This chapter delves into the leading IaC tools—Terraform, Ansible, Kubernetes, and OpenStack—and provides detailed examples and sample code to illustrate their application in 5G network deployment.

7.1. Terraform

Terraform by **HashiCorp** is a powerful, open-source IaC tool that uses a declarative approach to define and provision infrastructure. Terraform is particularly suited for multi-cloud deployments, making it an ideal choice for 5G operators who require a flexible solution to manage infrastructure across public and private cloud environments [34].

7.1.1. Key Features

- **Declarative Syntax**: Users specify the desired state of their infrastructure, and Terraform determines the steps to take to achieve it.
- **Multi-Cloud Support**: Works seamlessly across major cloud providers (e.g., AWS, Azure, Google Cloud), enabling hybrid 5G deployments.
- **State Management**: Maintains the state of deployed infrastructure, allowing for easy tracking and updates.

7.1.2. Sample Code for Deploying a 5G RAN Node

```
provider "aws" {
 region = "us-west-2"
}

resource "aws_instance" "5g_ran_node" {
 ami = "ami-0c55b159cbfafe1f0" # Example AMI ID for a base
instance
 instance_type = "t2.large"
 tags = {
 Name = "5G_RAN_Node"
 }

 provisioner "remote-exec" {
 inline = [
 "sudo apt-get update",
 "sudo apt-get install -y ran-software-package"
 ]
 }
}
```

The above code defines a simple configuration for deploying a 5G RAN node on AWS. It provisions an instance with specified tags and runs commands to set up necessary software.

7.1.3. Terraform has several use cases in 5G inlcuding

- **Multi-Region 5G Deployments**: Terraform can be used to deploy DUs and CUs across multiple cloud regions, supporting seamless scaling and failover capabilities.

7.2. Ansible

Ansible by Red Hat is an agentless IaC tool that excels in configuration management, application deployment, and orchestration. It uses an imperative approach, providing granular control over the steps taken during deployment. Ansible's simple YAML-based syntax makes it highly accessible and easy to integrate into CI/CD pipelines for 5G infrastructure management [35].

7.2.1. Key Features:

- **Agentless Architecture**: Uses SSH or WinRM to manage nodes, reducing overhead.
- **Idempotency**: Ensures that running the same playbook multiple times results in the same system state.
- **Extensive Module Library**: This library offers modules for managing cloud services, containers, and network equipment, ideal for 5G RAN and Core configurations.

7.2.2. Below is a sample code for configuring a 5G Core Network Function:

```
- name: Configure 5G Core Network Function
 hosts: core_network
 become: yes
 tasks:
 - name: Install required packages
 apt:
 name: "{{ item }}"
 state: present
 with_items:
 - upf-software
 - amf-software

 - name: Configure UPF
 copy:
```

```
 src: /templates/upf-config.yaml
 dest: /etc/5g-core/upf-config.yaml

 - name: Start UPF Service
 systemd:
 name: upf-service
 state: started
 enabled: yes
```

--- [36]

The Ansible playbook installs the necessary software for the User Plane Function (UPF) and Access and Mobility Management Function (AMF), copies configuration files, and starts the UPF service.

This scripting is practical in Automated Core Network Configuration. Ansible can manage the setup and configuration of network functions such as AMF and SMF in the 5G Core, ensuring consistent deployments across different environments.

7.3. Kubernetes

Kubernetes (K8s) is an open-source platform for automating containerized applications' deployment, scaling, and management. It is highly relevant in 5G network deployments, particularly for the Core and edge computing layers, where containerized Network Functions (NFs) and microservices play a crucial role.

7.3.1. Key Features in K8s

- **Container Orchestration**: Manages containers at scale, deploying network functions and microservices essential for the 5G Core.
- **Self-Healing**: Automatically restarts failed containers, reschedules disrupted services, and kills unresponsive containers.
- **Scalability**: Supports the horizontal scaling of NFs, ensuring that 5G networks can handle dynamic loads effectively.

7.3.2. An example of a Code for Deploying a Containerized AMF

```
provider "aws" {
 region = "us-west-2"
}

resource "aws_instance" "5g_ran_node" {
 ami = "ami-0c55b159cbfafe1f0" # Example AMI ID for a base
instance
 instance_type = "t2.large"
 tags = {
 Name = "5G_RAN_Node"
 }

 provisioner "remote-exec" {
 inline = [
 "sudo apt-get update",
 "sudo apt-get install -y ran-software-package"
 ]
 }
}
```

[37]

This Kubernetes deployment script defines an AMF (Access and Mobility Management Function) deployment with two replicas. The container runs the AMF software and mounts a configuration file for runtime parameters.

7.3.3. K8s has several use cases in 5G and network deployments including:

- **Edge Computing**: Kubernetes can orchestrate microservices at the network edge, ensuring that latency-sensitive applications like AR/VR and IoT devices receive efficient data processing.

7.4. OpenStack

OpenStack is an open-source cloud platform that supports Network Functions Virtualization (NFV), making it highly suitable for private cloud deployments in 5G networks. It provides a robust framework for managing large pools of compute, storage, and networking resources, facilitating the deployment of 5G Core and RAN components.

7.4.1. Key Features in OpenStack

- **NFV Support**: Integrates with VNFs to deliver flexible and scalable 5G network functions.
- **Multi-Tenancy**: This feature supports the isolation and management of resources across different slices of the network, aligning with 5G's network slicing capabilities.
- **Extensibility**: Offers a range of plug-ins and integrations to customize deployments for specific 5G use cases.

7.4.2. Sample Code for Deploying a Virtual Machine for a 5G Core Node

```
heat_template_version: 2018-08-31
description: Simple template to deploy a 5G Core Node

resources:
 5g_core_instance:
 type: OS::Nova::Server
 properties:
 image: 5g-core-image
 flavor: m1.large
 networks:
 - network: private-network
 user_data: |
 #!/bin/bash
 sudo apt-get update
 sudo apt-get install -y 5g-core-package
 key_name: my_key_pair
```

[38]

The above OpenStack Heat template deploys a virtual machine for a 5G Core Node, specifying the image, network, and configuration needed to install and start the 5G Core services.

7.4.3. OpenStack has several use cases, one of which is in:

- **Private Cloud for Core Network Deployment**: OpenStack provides a comprehensive solution for telecom operators looking to host their 5G Core on private infrastructure, offering complete control over resource allocation and security.

The use of Terraform, Ansible, Kubernetes, and OpenStack in 5G deployments illustrates the diverse toolkit available for managing different network components. Each tool serves unique purposes, from automated provisioning and configuration management to container orchestration and NFV support. By leveraging these IaC technologies, 5G network operators can ensure scalable, consistent, and agile infrastructure management, meeting the demands of modern telecommunications [39].

8. Case Studies and Real-World Implementations

Implementing Infrastructure-as-Code (IaC) in real-world 5G deployments provides valuable insights into how automated infrastructure management has transformed the telecommunications industry. This chapter highlights notable case studies that showcase successful IaC deployment in 5G infrastructure, emphasizing the lessons learned, challenges encountered, and best practices that emerged from these implementations.

8.1. Case Study 1: Large-Scale 5G RAN Deployment by a Global Telecom Provider

A leading global telecom operator undertook an ambitious project to deploy 5G Radio Access Network (RAN) infrastructure across multiple urban and suburban areas. The goal was to ensure rapid and consistent deployment of Distributed Units (DUs) and Centralized Units (CUs) to meet the high demand for 5G connectivity [40].

IaC Strategy: The telecom operator leveraged Terraform and Ansible to automate the provisioning and configuration of RAN components. Terraform created infrastructure templates that defined the physical and virtual resources required for DU and CU deployment, while Ansible handled the detailed configuration of network protocols and software updates.

8.1.1. What are the Implementation Highlights?

- **Automated Multi-Region Deployment**: The IaC approach enabled the operator to deploy RAN components in different geographical locations using consistent scripts. Terraform modules were adapted to account for regional differences in network topology and local regulations.
- **Configuration Uniformity**: Ansible playbooks ensured that all DUs and CUs were configured with standardized parameters, reducing the risk of configuration drift.

8.1.2. There are also Lessons to be Learned, a few of which are mentioned below

- **Modular IaC Code Enhances Scalability**: By using modular templates, the operator could scale the deployment seamlessly as demand increased. Reusable code blocks simplified the expansion of network coverage.
- **Continuous Monitoring Integration**: Integrating IaC with monitoring tools such as Prometheus enabled real-time tracking of deployment status and network health, allowing for quick identification and resolution of issues.

8.1.3. What Best Practices can be employed

- **Develop Modular IaC Templates**: Breaking down IaC scripts into smaller, reusable modules facilitates scalable and maintainable code that can adapt to different deployment scenarios.
- **Combine Declarative and Imperative Tools**: Using Terraform for infrastructure provisioning and Ansible for configuration management provided a balanced approach that enhanced flexibility and control.

8.2. Case Study 2: 5G Core Network Deployment by a Regional Telecom Operator

A regional telecom operator focused on modernizing its core network to support advanced 5G services, including network slicing and low-latency applications. The operator used IaC to deploy and manage key Network Functions (NFs) such as the User Plane Function (UPF) and Session Management Function (SMF) [41].

IaC Strategy: The operator employed Kubernetes and OpenStack for container orchestration and virtual infrastructure management. IaC scripts in Helm charts were used to deploy containerized NFs on Kubernetes, while OpenStack's Heat templates provisioned the underlying VMs and storage.

8.2.1. Implementation Highlights

- **Containerized Core Functions**: Deploying UPF and SMF as containerized microservices provided the flexibility to scale these functions independently based on traffic conditions.
- **CI/CD Integration**: IaC was integrated with a CI/CD pipeline using **Jenkins**, allowing the operator to automate the testing and deployment of new core network features.

8.2.2. Challenges Encountered

- **Complexity in Orchestration**: Managing the orchestration of multiple containerized functions with diverse performance requirements proved challenging, necessitating advanced configurations in Kubernetes.
- **Security Considerations**: Ensuring the secure storage of IaC scripts and related credentials was a priority, leading to adopting HashiCorp Vault for secrets management.

8.2.3. There are also Lessons to be Learned, a few of which are mentioned below

- **Robust CI/CD Pipelines Reduce Deployment Time**: Automating the testing and rollout of IaC scripts significantly reduced the time required to deploy new features, leading to faster delivery cycles and improved agility.
- **Monitoring and Observability Are Crucial**: Setting up observability tools like Grafana for visualizing real-time performance metrics proved essential for maintaining optimal service levels and preemptively addressing potential issues.

8.2.4. General best practices in IaC/CICD approach

- **Incorporate Secrets Management**: Ensuring that sensitive information in IaC scripts is securely managed reduces the risk of unauthorized access.
- **Use Helm for Simplified Deployment**: Helm charts streamlined the deployment of complex network functions, making them easier to version and maintain.

8.3. Case Study 3: Service-Based Interface (SBI) Deployment in a Multi-Vendor Environment

A European telecom operator was challenged to deploy a Service-Based Interface (SBI) to support interactions between multiple 5G Core functions in a multi-vendor environment. The goal was to ensure seamless communication between network functions sourced from different vendors while maintaining high availability [42].

IaC Strategy: The operator employed Ansible for API gateway configuration and Terraform to provision cloud infrastructure on Azure. The SBI deployment required customized IaC modules that could handle vendor-specific configurations while maintaining a unified deployment approach.

8.3.1. What are the implementation highlights from case studies?

- **Standardized API Configuration**: Ansible playbooks were created to configure API gateways uniformly, ensuring that all network functions, regardless of vendor origin, adhered to the same security and operational policies.
- **Cross-Vendor Compatibility**: Terraform modules were adapted to deploy infrastructure that could integrate with proprietary technologies from different vendors without compromising interoperability.

8.3.2. Challenges Encountered in IaC deployments in Multivendor environments

- **Compatibility Issues**: Compatibility between different vendors' APIs and protocols required significant customization of IaC scripts.
- **Regulatory Compliance**: Ensuring that the IaC deployment met regional data privacy laws and compliance standards added layer of complexity.

8.3.3. There are also Lessons to be Learned, a few of which are mentioned below

- **Customized IaC Enhances Flexibility**: Customizing IaC templates to accommodate vendor-specific requirements allowed the operator to maintain consistency across a heterogeneous environment.
- **Compliance Should Be Built into IaC**: Incorporating compliance checks directly into IaC scripts streamlined audits and ensured adherence to legal requirements.

8.3.4. Adoptable IaC Best Practices in a Multi-Vendor Environment

- **Develop Vendor-Agnostic IaC Templates**: Designing IaC templates that can be adapted for use with different vendors enhances flexibility and reduces deployment time [43].
- **Integrate Compliance Checks**: Including compliance validation within IaC scripts helps automate adherence to regulatory standards, making deployments more efficient [44].

These case studies underscore the transformative potential of IaC in 5G network deployments. Tools such as Terraform, Ansible, Kubernetes, and OpenStack have enabled telecom operators to deploy and manage complex 5G infrastructure efficiently [45]. Key lessons learned include the importance of modular IaC code, robust CI/CD pipeline integration, comprehensive security practices, and observability. By applying best practices such as modular code design, vendor-agnostic templates, and secrets management, telecom operators can overcome common challenges and achieve successful 5G deployments.

9. Future Trends and Research Opportunities

The infrastructure-as-code (IaC) landscape in 5G network deployment is continually evolving, driven by technological advancements and the growing need for efficient and scalable infrastructure management. Future trends and research opportunities focus on enhancing IaC's capabilities to keep pace with the dynamic requirements of 5G and beyond. This chapter explores key areas where innovation is likely to shape the future of IaC, including zero-touch automation, standardization efforts, and AI/ML integration for predictive management.

9.1. Zero-Touch Automation (ZTA): Enhancing IaC Frameworks for Minimal Human Intervention

Zero-touch automation represents the goal of infrastructure management, where IaC frameworks are enhanced to deploy, configure, and maintain network infrastructure with little to no human intervention [46]. This approach aligns with the concept of autonomous networks, which can self-manage and adapt to changes in network conditions in real-time.

9.1.1. Key Features and Benefits of ZTA

- **Self-Healing Infrastructure**: Future IaC frameworks will likely include self-healing capabilities, where infrastructure automatically detects and rectifies issues such as misconfigurations or resource failures without manual input. This reduces downtime and enhances reliability.
- **Automated Scaling and Load Management**: Zero-touch automation can enable infrastructure to scale dynamically based on network traffic and user demand. For example, IaC scripts integrated with AI-driven monitoring tools can anticipate traffic surges and preemptively deploy additional resources to maintain service quality [47].
- **Real-Time Updates and Patch Management**: IaC frameworks with zero-touch capabilities will automate the deployment of software patches and updates, ensuring that network functions remain secure and up to date without operator intervention.

9.1.2. ZTA Implementation Example

- **Closed-Loop Automation**: A system that uses telemetry data from monitoring tools like Prometheus can trigger IaC scripts automatically when predefined thresholds are met. For instance, if a User Plane Function (UPF) CPU usage exceeds a specific limit, the IaC framework could deploy additional UPF instances or allocate more resources.

9.1.3. ZTA Research Opportunities

- **Development of Autonomous IaC Platforms**: Research can focus on creating platforms that integrate IaC with Network Function Virtualization Orchestrators (NFVOs) and AI engines for fully autonomous deployments.
- **Intelligent Decision Algorithms**: Further exploration into AI algorithms that make real-time decisions based on infrastructure data to optimize resource allocation and network performance.

9.2. Standardization Efforts for IaC: Creating Universal Protocols for Better Vendor Compatibility

One of the significant challenges in 5G network deployments is the need for standardized protocols for IaC, particularly in multi-vendor environments [48]. Developing universal standards and protocols can simplify deployments, reduce complexity, and enhance compatibility across different vendor solutions.

9.2.1. Current Challenges include

- **Vendor-Specific Implementations**: Many IaC tools and frameworks are optimized for specific vendors or cloud providers, which can make deployment in heterogeneous environments challenging.
- **Fragmented Ecosystem**: Using multiple IaC tools without a common standard can result in fragmented infrastructures, making maintenance and scaling more complex.

9.2.2. Future Trends in IaC with ZTA

- **Unified IaC Templates and APIs**: Industry leaders are working on creating standardized templates and APIs that can be used across different tools and platforms. This would allow network operators to use the same IaC scripts for multiple vendors' hardware and software without significant modifications.
- **Collaboration with Standards Organizations**: Collaborations with bodies such as the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF) can drive the

development of open standards for IaC. These standards facilitate better interoperability between vendors and ensure consistency in deployments.

9.2.3. Research Opportunities in IaC as network convergence continues

- **Cross-Vendor IaC Frameworks**: Developing IaC frameworks that natively support multi-vendor integration with minimal custom code is a potential research avenue.

- Protocol Harmonization Studies: Research how existing protocols (e.g., NETCONF/YANG for network configurations) can be extended to serve as a universal language for IaC in 5G.

Example of Future Implementation: Imagine a unified IaC platform that leverages standardized modules compatible with cloud-native environments and legacy network infrastructure. Such a platform could deploy and manage DUs, CUs, core network functions, and edge nodes using a standard set of scripts, regardless of the vendor.

9.3. AI/ML Integration for Predictive IaC Management: Leveraging AI for Proactive Resource Management

Artificial Intelligence (AI) and Machine Learning (ML) are set to revolutionize IaC by enabling predictive infrastructure management. This integration allows for proactive decision-making, where the infrastructure can anticipate potential issues and make adjustment before they impact network performance.

9.3.1. Key Benefits of AI/ML in IaC

- **Predictive Scaling**: ML models trained on historical data can predict traffic patterns and trigger IaC scripts to scale network functions accordingly. This ensures that resources are available when needed, improving service quality and reducing latency.
- **Anomaly Detection**: AI can monitor infrastructure in real time and detect anomalies that may indicate security threats or potential system failures. By integrating these insights with IaC, automated corrective actions can be taken immediately.
- **Resource Optimization**: AI algorithms can analyze infrastructure usage data to optimize resource allocation, ensuring no component is over- or under-utilized. This leads to more efficient use of computing resources and cost savings.

9.3.2. Implementation Scenario of AI driven IaC

- **AI-Driven Monitoring with Automated IaC**: A telecom operator might use an AI-based platform to analyze metrics from 5G network functions. If the system detects an increase in latency or packet loss beyond acceptable levels, it triggers an IaC script to deploy additional resources or reroute traffic to maintain performance.
- **Dynamic Policy Adjustments**: ML models can continuously learn from network behavior and suggest or implement changes to infrastructure policies defined in IaC scripts, such as bandwidth allocation for different network slices.

9.3.3. Research Opportunities of AI in IaC

- **Advanced ML Models for Predictive Management**: Research could focus on developing ML models trained on diverse data sets to predict and respond to a wide range of network conditions.
- **AI-Enhanced IaC Frameworks**: Studies on embedding ML capabilities directly into IaC tools to create self-learning infrastructure management systems.
- **Explainable AI (XAI) for IaC**: Researching explainable AI techniques to ensure that the decisions made by AI/ML models are transparent and can be understood by network operators, fostering trust and easier troubleshooting.

Best Practices for Implementation xAI include training on comprehensive datasets, ensuring that ML models are trained on diverse and representative data sets to cover a wide range of network scenarios, and a hybrid approach by combining AI-driven automation with human oversight to balance proactive management with strategic input.

The future of IaC in 5G deployment promises significant advancements driven by zero-touch automation, standardization efforts, and the integration of AI/ML for predictive infrastructure management. These trends will make IaC more autonomous, scalable, and compatible across multi-vendor ecosystems, further enhancing the efficiency and reliability of 5G networks. Ongoing research and development in these areas will be crucial to overcoming current limitations and pushing the boundaries of what IaC can achieve in modern telecommunications.

10. Conclusion

Infrastructure-as-Code (IaC) has firmly established itself as an indispensable tool for the deployment and management of complex 5G infrastructure, encompassing the Radio Access Network (RAN), Core Network, and Service-Based Interface (SBI). Its capacity to transform traditionally manual and resource-intensive processes into automated, efficient, reproducible operations has redefined how 5G networks are developed and maintained. Through declarative and imperative scripting, IaC enables network operators to achieve scalable, consistent, and flexible infrastructure management that aligns with the rapid evolution of 5G services and user expectations [49].

IaC has been essential in modernizing the deployment processes of 5G infrastructure by automating the provisioning, configuration, and lifecycle management of network components [50]. In the RAN, IaC supports the automated deployment of Distributed Units (DUs) and Centralized Units (CUs), which are critical for achieving seamless coverage and low-latency connectivity [50]. For the 5G Core Network, IaC simplifies the deployment of complex network functions, such as the User Plane Function (UPF) and Session Management Function (SMF), through containerized microservices and virtualization techniques. In the SBI, IaC ensures the consistent configuration of APIs and the management of inter-function communication, supporting the modular and scalable nature of the 5G Core [50].

Case studies have demonstrated that IaC implementation can accelerate 5G rollouts, improve consistency, and reduce the risk of human error. By integrating with CI/CD pipelines, network operators have realized faster deployments and updates with minimal disruption. Additionally, multi-vendor environments, often seen as a complex challenge, have been successfully managed using tailored IaC scripts that standardize deployment while accommodating vendor-specific variations.

The benefits of IaC are multifaceted, including enhanced scalability and flexibility for infrastructure that must respond dynamically to varying traffic loads. IaC scripts help network operators adjust resources in real time by automating scaling operations and supporting applications such as augmented reality (AR) and massive IoT deployments. Operational cost reduction is another significant advantage, as automated processes reduce the need for extensive manual intervention and the associated labor costs [51].

The consistency and reliability offered by IaC help maintain uniform configurations across distributed network components, preventing configuration drift and ensuring that services meet quality standards. Integrating IaC with CI/CD pipelines accelerates the rollout of new features and patches and strengthens the resilience of the 5G network by automating testing and validation processes before deployment.

10.1. Challenges and Future Directions

Despite its transformative benefits, deploying IaC in 5G infrastructure is challenging. Complexity in multi-vendor environments requires IaC frameworks to be highly adaptable and capable of seamlessly integrating proprietary tools and configurations. Security concerns, such as the potential exposure of sensitive information within IaC scripts, must be managed through best practices, including using secrets management tools like HashiCorp Vault.

Another notable challenge is orchestrating and managing network slicing, which necessitates sophisticated IaC scripts capable of deploying and maintaining multiple logical networks with distinct QoS requirements. Compliance with regulatory standards adds another layer of complexity, requiring IaC scripts to be flexible enough to meet various regional data protection and sovereignty laws [52].

Looking ahead, future trends point towards further advancements that will enhance the capabilities and adoption of IaC in 5G. Zero-touch automation represents a significant leap forward, aiming for infrastructure that self-deploys, self-heals, and self-updates with minimal human intervention. This level of automation aligns with the broader industry move towards autonomous networks, where AI and machine learning play critical roles in predictive management and anomaly detection.

Standardization efforts are also expected to accelerate, fostering the creation of universal IaC templates and protocols that simplify deployments across multi-vendor ecosystems. Collaboration with standards organizations like ETSI and IETF will be essential in driving the development of consistent, vendor-agnostic IaC practices. Integrating AI/ML for predictive IaC management promises to enhance proactive resource allocation and real-time decision-making, ensuring that network performance is optimized continuously.

The future of IaC in telecommunications holds immense promise, with research focusing on creating autonomous, self-optimizing IaC frameworks that can seamlessly integrate with evolving 5G architectures and beyond. By incorporating AI capabilities directly into IaC platforms, network operators can leverage predictive analytics for more intelligent, more adaptive infrastructure management. The shift towards explainable AI (xAI) will ensure that automated decisions are transparent and understandable, promoting trust and operational clarity [53].

While security, interoperability, and regulatory compliance challenges remain, the continuous improvement of IaC tools, best practices, and research into emerging technologies will drive the industry forward. As 5G networks expand and become more complex, the role of IaC will become even more critical in delivering scalable, efficient, and reliable telecommunications services. The robust future of IaC in the telecommunications industry will be shaped by its ability to evolve and adapt, meeting the demands of increasingly sophisticated network infrastructures while supporting the innovation and growth that 5G promises to deliver

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] M. Zieba, M. Natkaniec, and P. Borylo, "Cloud-Enabled Deployment of 5G Core Network with Analytics Features," *Appl. Sci.*, vol. 14, no. 16, 2024. [Online]. Available: https://www.mdpi.com/2076-3417/14/16/7018

[2] T. Geier, "Improving Multi-Tenant I/O-Acceleration for Containerized Network Function Environments," in *NOMS 2024 - IEEE Network Operations and Management Symposium*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10575178/

[3] S. Maitra, T. O. Atalay, and A. Stavrou, "Towards Shielding 5G Control Plane Functions," in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2024. [Online]. Available: https://dsn2024uq.github.io/Proceedings/pdfs/DSN2024-6rvE3SSpzFYmysif75Dkid/410500a302/410500a302.pdf

[4] J. D. Guerrero-Balaguera, J. E. R. Condia, "Evaluating the Reliability of Supervised Compression for Split Computing," in *2024 IEEE 42nd Conference*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10538938/

[5] D Olufemi, "AI-enhanced predictive maintenance systems for critical infrastructure: Cloud-native architectures approach," 2024. [Online]. Available: https://wjaets.com/sites/default/files/WJAETS-2024-0552.pdf

[6] F. Gorlero, "Tapping Encrypted Traffic in a Kubernetes Cluster Using Sidecar-based Service Mesh," *Master's Thesis*, Politecnico di Torino, 2024. [Online]. Available: https://webthesis.biblio.polito.it/33338/

[7] V. Charpentier and N. Slamnik-Kriještorac, "Next-Gen Connectivity: Dynamic QoS Optimization for 5G Standalone and Vertical Integration," in *IEEE Conference on Smart Systems and Internet of Things*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10620807/

[8] R. Cavalcanti, "The Rise of The Machines: Fuzzing Framework for Security Tests of 5G User Equipment," *PhD Thesis*, University of Coimbra, 2024. [Online]. Available: https://estudogeral.uc.pt/handle/10316/116584

[9] A. A. Abd El-Latif, L. Tawalbeh, and Y. Maleh, *Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities*, 2024. [Online]. Available: https://books.google.com/books?hl=en&id=cF78EAAAQBAJ

[10] T. Hammouchi, D. Rupprecht, and K. S. Kohls, "Intrusion Detection System for 5G Core Systems," *Bachelor's Thesis*, Radboud University, 2023. [Online]. Available: https://www.cs.ru.nl/bachelors-theses/2024/Taha_Hammouchi___1044787___Intrusion_Detection_System_for_5G_Core_Systems.pdf

[11] J. P. N. Rodrigues, "Open Source Non-public 5G Networking in Licensed and Unlicensed Bands," *MSc Thesis*, University of Porto, 2023. [Online]. Available: https://repositorio-aberto.up.pt/bitstream/10216/153247/2/645875.pdf

[12] Y. S. Liu, S. Qi, P. Y. Lin, and H. S. Tsai, "L25GC+: An Improved, 3GPP-compliant 5G Core for Low-latency Control Plane Operations," in *2023 IEEE 12th Int. Conf. on Computing and Communications*, 2023. [Online]. Available: https://shixiongqi.github.io/_pages/papers/l25gc+.pdf

[13] F. Dolente, R. G. Garroppo, and M. Pagano, "A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions," *Future Internet*, vol. 16, no. 1, 2023. [Online]. Available: https://www.mdpi.com/1999-5903/16/1/1/pdf

[14] S. Aldas and A. Babakian, "Cloud-Native Service Mesh Readiness for 5G and Beyond," *IEEE Access*, 2023. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/10005208/10327727.pdf

[15] P. A. Assorow, "Research on 5G Core Network Slicing and Its Associated Security Issues," *MSc Thesis*, University of Alberta, 2023. [Online]. Available: https://era.library.ualberta.ca/items/703ca7d4-bec2-4d5f-bce0-03f6c188bac4

[16] D Bobie-Ansah , D Olufemi , E Agyekum Kyewaa, " Adopting Infrastructure as Code as A Cloud Security Framework for Fostering an Environment of Trust and Openness to Technological Innovation Among Businesses: Comprehensive Review," *INIS Database*, 2023. [Online]. Available: https://www.ijrti.org/viewpaperforall?paper=IJRTI2408026

[17] Q. Wang and Y. Rao, "Enhancing Smart Park Infrastructure through the Implementation of a Comprehensive Travel Chain System Based on Autonomous Driving," in *2023 5th International Symposium on Smart Infrastructure*, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10545626/

[18] E. Zeydan, J. Mangues-Bafalluy, and J. Baranda, "Service Based Virtual RAN Architecture for Next Generation Cellular Systems," in *IEEE Conf. on Communications Workshops*, 2022. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/6514899/09684900.pdf

[19] L. Zhao, M. M. Bala, W. Gang, and P. Chengkang, "A Survey on Open-Source-Defined Wireless Networks: Framework, Key Technology, and Implementation," *arXiv preprint arXiv:2209.01891*, 2022. [Online]. Available: https://arxiv.org/pdf/2209.01891

[20] Q. Tang, O. Ermis, C. D. Nguyen, and A. De Oliveira, "A Systematic Analysis of 5G Networks with a Focus on 5G Core Security," *IEEE Commun. Mag.*, 2022. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/9668973/09709835.pdf

[21] M. Zieba, M. Natkaniec, and P. Borylo, "Cloud-Enabled Deployment of 5G Core Network with Analytics Features," *Applied Sciences*, vol. 14, no. 16, 2024. [Online]. Available: https://www.mdpi.com/2076-3417/14/16/7018

[22] G. Gemmi, M. Segata, and L. Maccari, "Estimating Coverage and Capacity of High Frequency Mobile Networks in Ultra-dense Urban Areas," *Computer Communications*, 2024. [Online]. Available: https://iris.unitn.it/bitstream/11572/410299/1/comcomvsi.pdf

[23] F. Gorlero, "Tapping Encrypted Traffic in a Kubernetes Cluster Using Sidecar-based Service Mesh," *Master's Thesis*, Politecnico di Torino, 2024. [Online]. Available: https://webthesis.biblio.polito.it/33338/

[24] V. Charpentier and N. Slamnik-Kriještorac, "Next-Gen Connectivity: Dynamic QoS Optimization for 5G Standalone and Vertical Integration," in *IEEE Conference on Smart Systems and Internet of Things*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10620807/

[25] T. Geier, "Improving Multi-Tenant I/O-Acceleration for Containerized Network Function Environments," in *NOMS 2024 - IEEE Network Operations and Management Symposium*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10575178/

[26] S. Maitra, T. O. Atalay, and A. Stavrou, "Towards Shielding 5G Control Plane Functions," in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2024. [Online]. Available: https://dsn2024uq.github.io/Proceedings/pdfs/DSN2024-6rvE3SSpzFYmysif75Dkid/410500a302/410500a302.pdf

[27] R. Cavalcanti, "The Rise of The Machines: Fuzzing Framework for Security Tests of 5G User Equipment," *PhD Thesis*, University of Coimbra, 2024. [Online]. Available: https://estudogeral.uc.pt/handle/10316/116584

[28] Y. S. Liu, S. Qi, P. Y. Lin, and H. S. Tsai, "L25GC+: An Improved, 3GPP-compliant 5G Core for Low-latency Control Plane Operations," in *2023 IEEE 12th International Conference on Computing and Communications*, 2023. [Online]. Available: https://shixiongqi.github.io/_pages/papers/l25gc+.pdf

[29] F. Dolente, R. G. Garroppo, and M. Pagano, "A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions," *Future Internet*, vol. 16, no. 1, 2023. [Online]. Available: https://www.mdpi.com/1999-5903/16/1/1/pdf

[30] T. Hammouchi, D. Rupprecht, and K. S. Kohls, "Intrusion Detection System for 5G Core Systems," *Bachelor's Thesis*, Radboud University, 2023. [Online]. Available: https://www.cs.ru.nl/bachelors-theses/2024/Taha_Hammouchi___1044787___Intrusion_Detection_System_for_5G_Core_Systems.pdf

[31] J. P. N. Rodrigues, "Open Source Non-public 5G Networking in Licensed and Unlicensed Bands," *MSc Thesis*, University of Porto, 2023. [Online]. Available: https://repositorio-aberto.up.pt/bitstream/10216/153247/2/645875.pdf

[32] P. A. Assorow, "Research on 5G Core Network Slicing and Its Associated Security Issues," *MSc Thesis*, University of Alberta, 2023. [Online]. Available: https://era.library.ualberta.ca/items/703ca7d4-bec2-4d5f-bce0-03f6c188bac4

[33] T. Roha, C. T. Han, S. W. Y. Wan, A. Z. Nur, and S. A. S. Muhammad, "A Pilot Study of Radiofrequency Electromagnetic Fields Radiation Exposure Emits by the 5G Radio Communication Infrastructure in Kuala Lumpur," *INIS Database*, 2023. [Online]. Available: https://inis.iaea.org/search/search.aspx?orig_q=RN:54122356

[34] S. Aldas and A. Babakian, "Cloud-Native Service Mesh Readiness for 5G and Beyond," *IEEE Access*, 2023. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/10005208/10327727.pdf

[35] Q. Wang and Y. Rao, "Enhancing Smart Park Infrastructure through the Implementation of a Comprehensive Travel Chain System Based on Autonomous Driving," in *2023 5th International Symposium on Smart Infrastructure*, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10545626/

[36] E. Zeydan, J. Mangues-Bafalluy, and J. Baranda, "Service Based Virtual RAN Architecture for Next Generation Cellular Systems," in *IEEE Conf. on Communications Workshops*, 2022. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/6514899/09684900.pdf

[37] L. Zhao, M. M. Bala, W. Gang, and P. Chengkang, "A Survey on Open-Source-Defined Wireless Networks: Framework, Key Technology, and Implementation," *arXiv preprint arXiv:2209.01891*, 2022. [Online]. Available: https://arxiv.org/pdf/2209.01891

[38] Q. Tang, O. Ermis, C. D. Nguyen, and A. De Oliveira, "A Systematic Analysis of 5G Networks with a Focus on 5G Core Security," *IEEE Commun. Mag.*, 2022. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/9668973/09709835.pdf

[39] T. Geier, "Improving Multi-Tenant I/O-Acceleration for Containerized Network Function Environments," in *NOMS 2024 - IEEE Network Operations and Management Symposium*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10575178/

[40] S. Maitra, T. O. Atalay, and A. Stavrou, "Towards Shielding 5G Control Plane Functions," in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2024. [Online]. Available: https://dsn2024uq.github.io/Proceedings/pdfs/DSN2024-6rvE3SSpzFYmysif75Dkid/410500a302/410500a302.pdf

[41] J. D. Guerrero-Balaguera and J. E. R. Condia, "Evaluating the Reliability of Supervised Compression for Split Computing," in *2024 IEEE 42nd Conference*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10538938/

[42] G. Gemmi, M. Segata, and L. Maccari, "Estimating Coverage and Capacity of High Frequency Mobile Networks in Ultra-dense Urban Areas," *Computer Communications*, 2024. [Online]. Available: https://iris.unitn.it/bitstream/11572/410299/1/comcomvsi.pdf

[43] F. Gorlero, "Tapping Encrypted Traffic in a Kubernetes Cluster Using Sidecar-based Service Mesh," *Master's Thesis*, Politecnico di Torino, 2024. [Online]. Available: https://webthesis.biblio.polito.it/33338/

[44] V. Charpentier and N. Slamnik-Kriještorac, "Next-Gen Connectivity: Dynamic QoS Optimization for 5G Standalone and Vertical Integration," in *IEEE Conference on Smart Systems and Internet of Things*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10620807/

[45] R. Cavalcanti, "The Rise of The Machines: Fuzzing Framework for Security Tests of 5G User Equipment," *PhD Thesis*, University of Coimbra, 2024. [Online]. Available: https://estudogeral.uc.pt/handle/10316/116584

[46] A. A. Abd El-Latif, L. Tawalbeh, and Y. Maleh, *Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities*, 2024. [Online]. Available: https://books.google.com/books?hl=en&id=cF78EAAAQBAJ

[47] T. Hammouchi, D. Rupprecht, and K. S. Kohls, "Intrusion Detection System for 5G Core Systems," *Bachelor's Thesis*, Radboud University, 2023. [Online]. Available: https://www.cs.ru.nl/bachelors-theses/2024/Taha_Hammouchi___1044787___Intrusion_Detection_System_for_5G_Core_Systems.pdf

[48] J. P. N. Rodrigues, "Open Source Non-public 5G Networking in Licensed and Unlicensed Bands," *MSc Thesis*, University of Porto, 2023. [Online]. Available: https://repositorio-aberto.up.pt/bitstream/10216/153247/2/645875.pdf

[49] P. A. Assorow, "Research on 5G Core Network Slicing and Its Associated Security Issues," *MSc Thesis*, University of Alberta, 2023. [Online]. Available: https://era.library.ualberta.ca/items/703ca7d4-bec2-4d5f-bce0-03f6c188bac4

[50] T. Roha, C. T. Han, S. W. Y. Wan, A. Z. Nur, and S. A. S. Muhammad, "A Pilot Study of Radiofrequency Electromagnetic Fields Radiation Exposure Emits by the 5G Radio Communication Infrastructure in Kuala Lumpur," *INIS Database*, 2023. [Online]. Available: https://inis.iaea.org/search/search.aspx?orig_q=RN:54122356

[51] S. Aldas and A. Babakian, "Cloud-Native Service Mesh Readiness for 5G and Beyond," *IEEE Access*, 2023. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/10005208/10327727.pdf

[52] Q. Wang and Y. Rao, "Enhancing Smart Park Infrastructure through the Implementation of a Comprehensive Travel Chain System Based on Autonomous Driving," in *2023 5th International Symposium on Smart Infrastructure*, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10545626/

[53] E. Zeydan, J. Mangues-Bafalluy, and J. Baranda, "Service Based Virtual RAN Architecture for Next Generation Cellular Systems," in *IEEE Conf. on Communications Workshops*, 2022. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/6514899/09684900.pdf