World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Security implication of network slicing in 5g-Enabled IoT environment

Omoshalewa Anike Adeosun [1,*], Mobolaji Olakunle Fakeyede [2], Adeyemi Afolayan Adesola [3] Gbenga Akingbulere [4] and Dave Olamide Anifowoshe [5]

[1] *Applied Cybersecurity, Faculty of Computing, Engineering and Science, University of South Wales, Newport, UK*
[2] *Software Engineer, Chevron, Department of Information Technology, San Ramon, California, United States.*
[3] *Security Analyst, Computer Science Department, Stephen F. Austin State University, Nacogdoches, Texas, US.*
[4] *Software Engineer, Department of Enterprise R&D NetSec R&D, Palo Alto network, Santa Clara, California, US.*
[5] *Information System, Faculty of Science and Technology, National Open University, Lagos, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 24(03), 2359-2373

Publication history: Received on 18 November 2024; revised on 24 December 2024; accepted on 26 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.3.3966

Abstract

The Internet of Things (IoT) situation has changed drastically as a result of the deployment of 5G technology, that provides improved connectivity, scalability, and network slicing for service differentiation. The security implications of network slicing in 5G-enabled IoT systems are examined in this study, with a focus on the necessity of strong isolation measures. The contribution of important technologies like Network Function Virtualization (NFV) and Software-Defined Networking (SDN) to safe slice operation is assessed. The limitations of current methods are also addressed by a Dynamic Secure Isolation Framework (DSIF), which combines dynamic resource allocation, AI-driven threat detection, and Zero Trust Architecture to improve isolation and reduce vulnerabilities.

The investigation suggests new technologies like blockchain and quantum cryptography as viable solutions for the primary issues with secure slicing, including as cost, latency, and lifecycle complexity. The suggested framework lays the groundwork for upcoming IoT advancements by guaranteeing safe, scalable, and resilient slice operations. Proactive security measures should be prioritized, standardized standards should be developed together, and more research into economic isolation methods should be conducted. The security and dependability of 5G network slicing in IoT are improved by this study's findings.

Keywords: 5G Network Slicing; Secure Isolation; AI-Driven Security; Blockchain Security; Quantum Cryptography

1. Introduction

The advent of 5G technology represents a revolutionary step in mobile communication, marked by unparalleled data transmission rates, low latency, and support for a massive density of connected devices. Advanced technologies like network slicing, which enable the dynamic allocation of network resources to satisfy various service requirements, are the foundation of this revolutionary shift [1]. With network slicing, several virtual networks that are each customized for certain use cases can be established on a single physical infrastructure [2]. Network slicing, a key component of 5G, is well-positioned to meet the expanding needs of the Internet of Things, including applications like driverless cars, smart cities, and healthcare. Network slicing divides physical networks into discrete virtual slices by utilizing virtualization technologies as Software-Defined Networking (SDN) and Network Function Virtualization (NFV) [3]. Every slice functions autonomously, providing that the resources and services allotted to it are tailored to meet particular needs. A network slice intended for enhanced mobile broadband (eMBB) might prioritize high-throughput services like video streaming, whilst another slice supporting ultra-reliable low-latency communication (URLLC) might serve mission-critical applications [4].

* Corresponding author: Omoshalewa Anike Adeosun

SDN and NFV form the technological backbone of network slicing. SDN decouples network control functions from physical hardware, allowing centralized management and improved flexibility. NFV, on the other hand, transforms traditional hardware-based network functions into software-based equivalents, enabling scalable and customizable deployments within slices [5]. These capabilities not only enhance operational efficiency but also lay the foundation for innovative business models like Network-as-a-Service (NaaS) and Internet of Things (IoT). The Internet of Things is characterized by a vast ecosystem of interconnected devices that communicate and exchange data autonomously [6]. As IoT applications proliferate, they impose diverse and stringent requirements on underlying network infrastructures. Network slicing addresses these challenges by providing tailored connectivity solutions [7]. For example, a single physical network can simultaneously host slices for industrial IoT, requiring high reliability and low latency, and consumer IoT, prioritizing cost-efficiency and scalability. This capacity for customization not only enhances the performance of IoT deployments but also facilitates the coexistence of heterogeneous services. By allocating isolated resources to each slice, network slicing mitigates potential conflicts and ensures that critical applications are not disrupted by resource-intensive tasks in other slices [8].

While the integration of network slicing with IoT promises significant benefits, it also amplifies the security challenges associated with 5G [4]. IoT devices are inherently vulnerable due to limited computational resources and weak security measures, making them prime targets for cyberattacks [9]. The proliferation of IoT increases the attack surface of 5G networks, as compromised devices can be exploited to infiltrate network slices or disrupt their operations. The security implications are profound. Inter-slice communication introduces vulnerabilities that adversaries can exploit to gain unauthorized access, while weak isolation mechanisms may lead to resource leakage or service disruptions [9]. Additionally, the dynamic nature of 5G networks necessitates robust authentication and authorization protocols to secure slice lifecycles and prevent malicious intrusions [5].

The increasing reliance on network slicing in IoT amplifies the urgency to address its associated security risks. Existing studies highlight significant gaps, including insufficient isolation between slices, inadequate protection against denial-of-service (DoS) attacks, and vulnerabilities in lifecycle management [4]. Furthermore, emerging technologies like AI-driven orchestration introduce additional complexities, raising concerns about data privacy and the integrity of decision-making processes within slices [10].

Despite these challenges, there is a lack of comprehensive frameworks addressing the unique security demands of network slicing in IoT environments. This study seeks to bridge this gap by investigating the implications of network slicing on IoT security and proposing solutions to enhance isolation and resilience.

2. Methodology

Using a conceptual framework that synthesizes information from existing literature, a focused review of technical studies, conference proceedings, and articles was carried out on reliable sources that address the architecture, vulnerabilities, and enabling technologies for network slicing. The study's core themes were identified and examined, including isolation techniques, lifecycle management, and cutting-edge technologies like AI-driven security, Network Function Virtualization (NFV), and Software-Defined Networking (SDN).

The Dynamic Secure Isolation Framework (DSIF) was created to fill in the holes in the current frameworks based on the information acquired. This framework incorporates important concepts and technologies, such as Zero Trust Architecture (ZTA) for improved security, NFV for virtualized network functions, and SDN for centralized control. The framework was designed to offer efficient, safe, and scalable slicing for a variety of IoT applications. Its elements and design were conceptually validated by matching them to the requirements and difficulties mentioned in the literature review.

3. Literature review

3.1. 5G Network Slicing

5G network slicing is a transformative technology that enables the creation of multiple virtual networks on a shared physical infrastructure, each tailored to meet specific application requirements such as throughput, reliability, latency, and availability [11]. This enables 5G networks to cater to diverse applications like voice communication, video streaming, e-health, and vehicular communication without compromise [12]. Through focusing on a smaller set of use-case-specific requirements, network slicing offers a more efficient and feasible alternative to the traditional approach of designing one-size-fits-all networks.

This approach leverages key technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV) to provide flexible, scalable, and efficient network services [5]. SDN separates the control plane from the data plane, allowing centralized network management and facilitating dynamic resource allocation. This flexibility ensures that each slice can have unique configurations tailored to its specific use case. NFV, on the other hand, replaces traditional hardware-based network functions with virtualized, software-based equivalents. This transformation enables rapid deployment, scalability, and adaptability of network functions within each slice. Together, SDN and NFV form the centre point of network slicing, ensuring its efficiency and robustness [13] [14].

Network slicing allows operators to allocate resources dynamically, ensuring optimal performance for diverse use cases such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC) [15]. Each slice operates independently, providing customized services without interference from other slices, thus enhancing the overall network efficiency and user experience [5]. Each slice is composed of interconnected sub-slices, such as a Core Network (CN) sub-slice and a Radio Access Network (RAN) sub-slice, which work together seamlessly to deliver end-to-end services. This architecture ensures not only operational independence but also enhances security by isolating resources and services across slices [14]. For example, in a smart city environment, a single physical 5G network could simultaneously host slices for traffic management, public safety, and consumer IoT applications, each with unique performance and security requirements. The ability to create on-demand slices, combined with their independent control and management, allows service providers to optimize resource utilization and deliver tailored solutions to diverse user groups.

The implementation of network slicing involves several critical components, including the Network Slice Selection Function (NSSF), which ensures the appropriate slice is selected based on the service requirements, and the Network Slice Management Function (NSMF), which oversees the lifecycle management of slices [5]. These components work together to provide seamless and secure network operations. [5] provided an example of how the logical view of the network slice instance is mirrored for various service kinds, including IoT, eMBB, URLLC, and others (Fig.1).

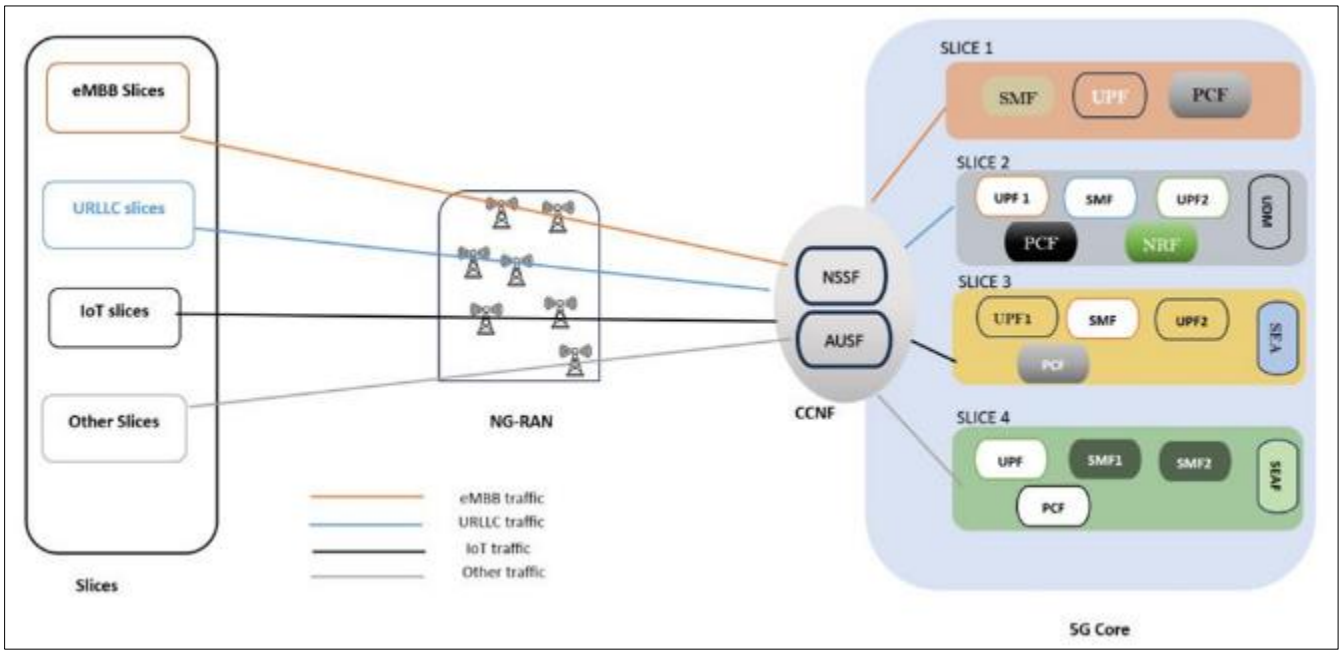

Figure 1 logical view of the network slice [5]

3.2. Architecture Design of 5G Network Slicing

The architecture of network slicing in 5G represents a fundamental shift in how telecommunication networks are designed and managed, to deliver a flexible, scalable, and service-specific framework [16]. Through the leveraging on the principles of virtualization, network slicing allows the creation of multiple logical networks that operate over shared physical infrastructure. This enables the seamless delivery of tailored services to meet diverse requirements, from high-speed internet for enhanced Mobile Broadband (eMBB) applications to ultra-reliable connectivity for industrial IoT use cases [17] [18].

At its core, the architecture is built upon three primary layers which are the resource layer, the network slice instance and the service instance layer. The resource layer encompasses the foundational components of the network, including both physical and virtualized resources [19]. These resources, such as processing nodes, storage units, and transmission elements, are managed dynamically to meet the demands of specific Network Slice Instances (NSIs). Critical network functions, such as routing, authentication, and slice selection, also reside within this layer, ensuring that the infrastructure is robust and adaptable to various service needs [20].

The second layer, the Network Slice Instance (NSI) layer, plays a pivotal role in enabling the flexibility and service customization promised by network slicing. An NSI represents a logical network configured to deliver specific services, comprising interconnected sub-slices that span the Radio Access Network (RAN), Transport Network (TN), and Core Network (CN) [21]. These sub-slices are not fixed in their proportions; instead, their configurations are tailored dynamically to align with the specific requirements of each use case. For instance, eMBB applications may utilize shared AMF (Access and Mobility Management Function) sub-slices to reduce signalling overhead, while industrial IoT applications requiring stringent data integrity may deploy exclusive core network sub-slices for enhanced security [18].

The service instance layer, the topmost layer, integrates the slices into cohesive service offerings for end-users. Abstracting the complexities of the underlying slicing technology, this layer ensures that service providers can deliver customized solutions without exposing customers to the intricate processes of slice management [22]. This makes network slicing particularly valuable in diverse domains such as virtual and augmented reality, e-health, and mission-critical industrial applications, where performance and reliability are paramount.

The architecture's flexibility is further enhanced by the seamless integration of virtualization technologies like Software-Defined Networking (SDN) and Network Function Virtualization (NFV). SDN decouples the control plane from the data plane, enabling centralized control and dynamic network configuration. NFV complements this by virtualizing traditional hardware-based functions, such as firewalls and load balancers, into software components. Together, these technologies enable on-demand creation, configuration, and management of network slices, ensuring that each slice operates independently and securely while sharing the same physical network [23].

An essential feature of this architecture is its ability to manage the lifecycle of network slices effectively. From the initial preparation and instantiation to real-time operation and eventual decommissioning, the architecture ensures that resources are optimally allocated and monitored. The slice manager plays a critical role in overseeing this lifecycle, coordinating with resource and service management functions to ensure smooth operation and high-quality service delivery [9].

In practice, the versatility of this architecture allows it to adapt to various application scenarios. For example, industrial IoT systems can use network slicing to ensure reliable and low-latency communication in environments like smart manufacturing. Similarly, in healthcare, the architecture supports applications such as telemedicine and remote surgery by guaranteeing high-bandwidth, low-latency connectivity. Each use case benefits from the architecture's ability to isolate resources and optimize service delivery without compromising the efficiency of the shared infrastructure [5].

The 5G network slicing architecture thus represents a significant evolution in network design, addressing the growing demand for diverse and specialized services. Combining robust resource management, dynamic slice configuration, and advanced virtualization technologies, this architecture provides a scalable and secure foundation for the future of telecommunications.

3.3. Lifecycle of a Network Slice

The lifecycle of a network slice consists of several distinct phases, each critical to the effective deployment and management of network slices within a 5G infrastructure. These phases include Preparation, Instantiation, Configuration and Activation, Run-time, and Decommissioning. Each phase encompasses specific tasks and objectives to ensure optimal performance and security of the network slices [9] [24] [5].

- **Preparation**: The preparation phase is dedicated to setting up the network environment and designing network slice templates. A network slice template is essentially a blueprint that outlines the components, structure, and configuration required for a specific slice. This phase involves the creation and modification of these templates, which serve as the foundation for building the slices in subsequent phases. The network environment is also prepared during this phase to ensure that all necessary resources and infrastructure are in place.

- **Instantiation, Configuration, and Activation:** In this phase, the network slice is instantiated based on the predefined template. This involves the creation, installation, and configuration of the necessary resources and network functions. The slice is built using specific instance information, ensuring that it meets the exact requirements outlined in the template. Once instantiated, the slice undergoes configuration and activation, making it operational and ready to provide the intended services.
- **Run-time:** During the run-time phase, the network slice is actively in use and can be subject to various modifications and adjustments. This phase involves continuous monitoring and supervision to ensure the slice operates efficiently and meets performance standards. Modifications such as upgrades, configuration changes, and the association or disassociation of resources and network functions may occur to adapt to changing requirements or to optimize performance. The slice manager plays a crucial role in this phase, overseeing the operational status and making necessary adjustments.
- **Decommissioning**: The final phase of the network slice lifecycle is decommissioning. Once the slice has fulfilled its service objectives, it is decommissioned to free up resources and network functions. This phase involves logging out the slice, effectively releasing the allocated resources, and dismantling the network functions associated with it. Post-decommissioning, the slice ceases to exist within the network environment.

Throughout these phases, the slice manager is instrumental in managing the lifecycle of the network slices. It is responsible for creating, configuring, and decommissioning slices, as well as mapping them to the required resources and functions. The slice manager interfaces with the network through a standardized Application Programming Interface (API), which allows for actions such as slice creation, deletion, configuration, and monitoring. Ensuring the security of the APIs and the overall lifecycle management processes is paramount to maintaining the integrity and reliability of the network slices.

4. Applications of Network Slicing in IoT

The integration of network slicing with IoT has unlocked a multitude of applications by providing customized connectivity and resource optimization. These applications cut across diverse sectors, leveraging the flexibility, low latency, and scalability of 5G-enabled IoT systems [18]. The International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP) have broadly categorized these use cases into three major categories: Ultra-Reliable Low-Latency Communication (URLLC), Enhanced Mobile Broadband (eMBB), and massive Machine-Type Communication (mMTC) [25] [26] [27].

- **Smart Cities**: Network slicing facilitates the deployment of interconnected systems in smart cities, enabling efficient traffic management, public safety, and environmental monitoring. By creating dedicated slices for high-priority applications such as emergency response, cities can ensure real-time data exchange and reliability while managing resources efficiently.
- **Healthcare and Telemedicine**: Healthcare systems benefit significantly from network slicing, particularly in telemedicine and remote patient monitoring. Dedicated slices ensure the high-speed, low-latency connectivity needed for real-time video consultations, medical data transfer, and remote surgical procedures, enhancing healthcare access and reducing dependency on physical consultations.
- **Industrial IoT (IIoT):** In manufacturing and industrial automation, network slicing supports URLLC, which is critical for precision-driven applications like robotics and factory automation. It also ensures data integrity and secure communication in high-stakes environments, such as chemical production or metal processing.
- **Transportation and Autonomous Vehicles:** Network slicing enables the seamless operation of autonomous vehicles and connected transportation systems. The dedication of slices to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, slicing ensures uninterrupted data flow for navigation, traffic updates, and collision prevention systems.
- **Smart Homes and Consumer IoT:** For consumer IoT applications, network slicing supports smart home devices like thermostats, security systems, and wearables. Dedicated slices optimize connectivity for low-power devices, ensuring consistent performance without interfering with other high-demand applications on the network.
- **Agriculture:** Precision agriculture leverages IoT devices for real-time monitoring of soil conditions, weather, and crop health. Network slicing enables the deployment of resource-efficient slices dedicated to such sensors, facilitating cost-effective and reliable agricultural solutions in remote areas.
- **Retail and Logistics:** The retail sector benefits from IoT applications like inventory management and smart payment systems, while logistics operations utilize IoT for tracking and optimizing delivery routes. Network slicing ensures these systems operate seamlessly, supporting dynamic scalability and reliability under varying workloads.

- **Edge Computing and AR/VR:** Dedicated slices for edge computing services, high-quality media streaming, and applications in augmented reality (AR) and virtual reality (VR) enhance user experiences by providing high bandwidth and low latency. These slices ensure smooth and reliable connectivity for data-intensive applications.
- **V2X Communication**: Vehicle-to-everything (V2X) communication, including V2V, V2I, and vehicle-to-pedestrian (V2P), benefits from network slicing by ensuring reliable and real-time data transmission, essential for the safety and efficiency of autonomous vehicles.
- **Smart Healthcare:** Smart healthcare applications, including remote monitoring and advanced telehealth services, leverage network slices to provide secure and reliable connectivity. This ensures critical health data is transmitted with minimal latency, improving patient outcomes and healthcare delivery.

The flexibility of network slicing allows operators to allocate resources dynamically and efficiently, catering to the specific needs of various IoT applications. This enables the smooth operation of smart cities, industrial automation, and other IoT-driven ecosystems, ultimately enhancing performance and user experience.

4.1. Advantages of Network Slicing for IoT

The advantages of network slicing in IoT are numerous, directly addressing the challenges posed by traditional network architectures. These benefits include:

- **Resource Optimization:** Network slicing maximizes resource utilization by dynamically allocating bandwidth, computing power, and storage based on specific application requirements [28]. This approach reduces wastage and ensures that critical applications receive priority resources.
- **Improved Scalability:** As IoT ecosystems expand, network slicing allows operators to scale resources effectively. New slices can be created on-demand, enabling the seamless integration of additional devices and applications without overburdening existing infrastructure.
- **Enhanced Performance and Reliability:** By isolating applications into dedicated slices, network slicing minimizes interference and latency [27]. This isolation ensures consistent performance, particularly for mission-critical applications like healthcare, autonomous vehicles, and industrial automation.
- **Security and Privacy:** The segmentation of network resources enhances security by isolating sensitive applications. For instance, industrial systems or healthcare data can be safeguarded against cyber threats through dedicated and monitored slices, reducing the risk of breaches.
- **Cost Efficiency:** Operators can leverage network slicing to offer Network-as-a-Service (NaaS), creating new revenue streams while providing cost-effective solutions. IoT service providers can deploy applications without the need for standalone infrastructure, reducing upfront investment and operational costs.
- **Support for Diverse Use Cases:** The ability to customize slices allows IoT applications to operate with unique configurations. From low-power sensors in agriculture to high-speed data requirements in entertainment, network slicing accommodates varying needs, ensuring service quality across domains.
- **Future-Proofing IoT Systems:** With the rapid evolution of IoT technologies, network slicing offers a scalable and adaptable solution to accommodate emerging applications and demands. This ensures that networks can evolve without requiring complete overhauls, saving time and resources.

5. Security Implications of Network Slicing in 5G IoT

Network slicing in 5G technology provides flexibility and efficiency by creating virtual networks tailored to specific use cases. While this innovation enables better resource allocation and the coexistence of multiple services on shared infrastructure, it also introduces several security risks. These challenges are particularly significant in the Internet of Things (IoT) ecosystem, where the interconnectedness of devices amplifies potential vulnerabilities [29]. Addressing the security implications of network slicing in 5G-enabled IoT is crucial to ensure reliable, efficient, and safe operations.

5.1. Threat Vectors in Network Slicing

5G network slicing is susceptible to various threat vectors that can compromise the security of the network. Among these, Denial of Service (DoS) attacks, misconfiguration attacks, and Man-in-the-Middle (MITM) attacks are particularly significant [30].

- **Denial of Service (DoS) Attacks:** DoS attacks pose a significant threat to the availability of network slices through overwhelming signalling planes or other critical components rendering the network slices unavailable. In 5G networks, such attacks can compromise access to remote data or disrupt essential communication

services. These attacks target the core functionality of slices, rendering IoT devices unable to perform their tasks effectively, resulting in loss of access to 5G infrastructure, remote data, and compromised communication services [29].

- **Misconfiguration Attacks:** Misconfiguration of system controls, such as inadvertently disabling security features, exposes slices to adversaries who exploit these weaknesses to gain unauthorized access. This can lead to significant breaches in confidentiality, integrity, and availability. Misconfigured slices may inadvertently enable attackers to manipulate or disable IoT services entirely.
- **Man-in-the-Middle (MITM) Attacks:** MITM attacks allow adversaries to intercept and alter communications between endpoints. Within 5G IoT, such attacks can result in data theft, misinformation, and disinformation, potentially compromising critical IoT applications like healthcare monitoring or autonomous vehicle communication [31].

5.2. Security Challenges Across the Slicing Lifecycle

The security vulnerabilities in network slicing manifest across its lifecycle: deployment, activation, operation, and decommissioning [5].

- Deployment Phase: The flexibility of network slicing allows the dynamic allocation of network elements (NEs), but this also opens up risks like DoS attacks, hypervisor hijacking, and side-channel attacks. In other words, the main security concerns include the potential introduction of flaws within the slice templates or the accidental introduction of malware [9]. Poorly designed slices or compromised templates can lead to data leakage and exposure of sensitive information once the slices are deployed. For example, during NE registration, attackers could use plaintext transmissions of registration information to inject malicious elements into the core network, compromising data confidentiality and operational integrity.
- Activation Phase: Attacks could target APIs used for slice activation. Network integrity may be jeopardized or services may be interrupted by fraudulent slices or altered configurations. Vulnerabilities during this stage could be used by attackers to disrupt services or intercept private IoT data [9].
- Operational Phase: In this phase, slices interact directly with IoT devices and other slices, creating opportunities for DoS, side-channel attacks, and unauthorized deletion of slices. A compromised slice could infect others or extract sensitive information. Effective isolation between slices is critical to prevent such lateral movement of threats [29].
- Decommissioning Phase: Improper deactivation of slices can leave residual sensitive data that attackers may exploit. This can result in data breaches or the reuse of stale data for malicious purposes, emphasizing the need for robust data destruction protocols during slice decommissioning [9].

5.3. Communication-Related Security Risks

Network slicing involves both intra-slice and inter-slice communication, each presenting its own set of security challenges.

- Intra-Slice Communication: Communications within a slice involves interactions among its sub-slices i.e. involving the exchange of data and signaling among different network functions (NFs) such as between components managing radio resources and edge computing [32]. The security of the entire slice often hinges on the weakest sub-slice. A compromise in one sub-slice can jeopardize the entire network, leading to service degradation or breaches in IoT data integrity [32] [9].
- Inter-Slice Communication: Collaboration between slices is necessary for delivering integrated IoT services. However, this interdependence introduces risks like unauthorized access or data tampering. Attackers may exploit these interactions to propagate threats across slices, making robust inter-slice security protocols essential [29].

5.4. Management-Related Threats

Management systems, including NSSMF (Network Slice Subnet Management Function) and NSMF (Network Slice Management Function), oversee the allocation of resources and control the lifecycle of slices. These systems are highly vulnerable to threats like unauthorized access, insider attacks, and configuration errors [9] [33].

- **DoS Attacks on Management Systems**: Such attacks can render management systems inoperable, leading to widespread service outages.
- **Insider Threats**: Authorized personnel may inadvertently or intentionally misconfigure slices, leading to vulnerabilities.

- **Vulnerable APIs and Protocols**: Attackers may exploit flaws in management APIs to gain unauthorized control over slices, compromising the security of IoT services.
- **End-Device Vulnerabilities**: End devices, such as IoT sensors, smart appliances, and industrial controllers, are the entry points for many attacks. These devices often operate with minimal security, making them susceptible to threats like malware injection and unauthorized access.
- **Device-Level Compromises**: A single compromised device can act as a gateway for attackers to infiltrate the network slice it is connected to, potentially affecting other devices and slices.
- **Data Breaches**: Sensitive IoT data, if not properly encrypted, can be intercepted and exploited, leading to privacy violations and operational disruptions

6. Ensuring Secure Isolation Between Slices

In 5G network slicing, ensuring secure isolation between slices is critical to maintaining the integrity, confidentiality, and availability of services provided by each slice [34]. Network slicing allows operators to offer customized virtual networks to meet the diverse needs of different IoT applications. However, this flexibility comes with the risk of cross-slice interference, where one slice could potentially affect or compromise another. To mitigate these risks, various isolation mechanisms are employed to ensure that each slice operates independently, without interference from other slices.

6.1. Isolation Mechanism

The primary goal of isolation in 5G network slicing is to ensure that slices can function independently, even when they share physical infrastructure. Several technologies enable this secure isolation, including Software-Defined Networking (SDN) and Network Function Virtualization (NFV), which are pivotal in managing resources and traffic efficiently [9].

- **Software-Defined Networking (SDN):** SDN is a network architecture approach that decouples the control plane from the data plane, allowing centralized management and dynamic configuration of network resources. In 5G network slicing, SDN provides an efficient means to create isolated virtual networks by defining policies that control the flow of traffic between slices. This ensures that data and resources allocated to one slice do not interfere with others. SDN controllers dynamically allocate and manage traffic flows, thus preventing unauthorized access and cross-slice contamination [35]. SDN's centralized control allows operators to enforce security policies across slices, detect potential security breaches in real-time, and reconfigure slices on-demand. For instance, if a particular slice is under attack or compromised, SDN controllers can isolate the affected slice and reroute traffic, ensuring that other slices remain unaffected.
- **Network Function Virtualization (NFV):** NFV enables the virtualization of network functions, allowing them to run on standard hardware rather than dedicated devices. This flexibility allows operators to create virtual instances of network functions (NF) within a slice, which can be isolated from other slices. Each virtual network function (VNF) operates independently, ensuring that the failure or compromise of one function does not affect others. Additionally, NFV supports dynamic resource scaling, which is essential for maintaining performance and security across slices [9]. NFV, when integrated with SDN, offers a powerful combination to isolate network functions and control traffic across slices [8]. NFV can dynamically spin up additional VNFs to manage increased traffic in a slice, ensuring that performance remains stable while maintaining isolation from other slices.

6.2. Comparative Analysis of Isolation Mechanisms

Table 1 Summary of key features and security benefits

Isolation Mechanism	Key Features	Security Benefits
SDN	Centralized control, dynamic resource allocation, policy enforcement	Enhanced traffic management, reduced attack surface, improved scalability
NFV	Virtualized network functions, flexible deployment, dynamic scaling	Isolation of network functions, resilience to failures, efficient resource utilization
Traditional Network Segmentation	Physical separation of network segments, static configuration	Strong isolation, limited flexibility, high cost
Containerization	Lightweight virtualization, rapid deployment, resource efficiency	Process-level isolation, reduced overhead, potential for cross-container attacks

To better understand the effectiveness of different isolation mechanisms, we can compare SDN and NFV with other approaches such as traditional network segmentation and containerization. The table below summarizes the key features and security benefits of each approach.

6.3. Existing Isolation Mechanisms

SDN and NFV: SDN and NFV are the cornerstone technologies for achieving secure isolation in 5G network slicing. SDN's centralized control plane allows for real-time monitoring and management of network traffic, enabling operators to detect and mitigate potential security threats quickly. By defining and enforcing traffic policies, SDN ensures that each slice remains isolated from others, preventing unauthorized access and data leakage.

NFV complements SDN by providing the flexibility to deploy and manage network functions as virtual instances. This virtualization ensures that each network function operates in its own isolated environment, reducing the risk of cross-slice attacks. NFV also supports the dynamic scaling of resources, allowing operators to allocate additional resources to slices as needed to maintain performance and security.

Traditional Network Segmentation: Traditional network segmentation involves physically separating network segments using dedicated hardware [36]. This method provides strong isolation but lacks the flexibility and scalability offered by SDN and NFV. It is costly to implement and difficult to adapt to changing demands or security threats. While traditional segmentation can ensure strong isolation, its inflexibility makes it less suitable for the dynamic needs of 5G network slicing

Containerization: Containerization is a lightweight virtualization approach that allows applications to run in isolated environments while sharing the same operating system kernel [37]. While containerization offers rapid deployment and resource efficiency, it introduces potential security risks, such as cross-container attacks. These risks can be mitigated through careful monitoring and the use of security policies that enforce strict isolation between containers. For 5G network slicing, containerization can be useful for resource-efficient slicing but requires additional security measures to prevent cross-container vulnerabilities.

7. Proposed Security Framework for 5G Network Slicing in IoT

The increasing adoption of 5G-enabled IoT calls for robust security measures to protect network slices from emerging threats. While existing frameworks such as SDN and NFV offer substantial benefits, they have limitations in addressing dynamic vulnerabilities, inter-slice dependencies, and the complexity of IoT environments. To overcome these shortcomings, an enhanced Dynamic Secure Isolation Framework (DSIF) tailored to address the security needs of 5G network slicing in IoT is proposed.

7.1. Architecture of the Framework

The DSIF is built on three layers, each designed to address specific security challenges:

- **Infrastructure Layer:** This layer represents the physical and virtual resources, including servers, routers, switches, and storage systems, supporting 5G slices. The resources are segmented into isolated zones using virtualized technologies such as SDN and NFV. Each zone is equipped with security modules for monitoring and controlling data flow, resource allocation, and access management.
- **Control and Orchestration Layer:** This middle layer centralizes the management of network slices and enforces security policies across the lifecycle of slices. It integrates a Zero Trust Security Module (ZTSM) and an Adaptive Threat Detection System (ATDS):
    - **ZTSM**: Ensures that all entities, including devices, users, and applications, are authenticated and authorized before accessing any slice.
    - **ATDS**: Uses AI-driven algorithms to monitor network behaviour in real time, identify anomalies, and respond proactively to potential threats.
- **Service and Application Layer:** This top layer hosts IoT applications and services running on individual slices. It uses end-to-end encryption and advanced access controls to ensure data confidentiality and integrity. Multi-layer firewalls and sandboxing techniques are used to secure inter-slice communication.

7.2. Operational Details

The DSIF framework operates dynamically, leveraging real-time monitoring, adaptive policy enforcement, and advanced threat mitigation strategies. Here's how it addresses key vulnerabilities:

7.2.1. Enhanced Isolation

- **Dynamic Resource Allocation**: SDN and NFV technologies are integrated with AI algorithms to monitor slice performance and allocate resources based on demand. This ensures that slices remain isolated, even during peak loads.
- **Micro-Segmentation**: Each slice is further divided into micro-segments, limiting the blast radius of an attack. If one micro-segment is compromised, the threat is contained, preventing lateral movement.

7.2.2. Mitigation of Vulnerabilities

- **API Security**: Secure APIs with Transport Layer Security (TLS) are implemented to prevent exploitation during slice activation and operation phases.
- **Anomaly Detection**: The ATDS identifies unusual traffic patterns, such as those indicative of a Denial-of-Service (DoS) attack or unauthorized access attempts. Once detected, the system triggers automatic responses, such as isolating the affected slice or redirecting traffic.
- **Data Leakage Prevention**: End-to-end encryption is enforced for all inter-slice and intra-slice communications. This ensures that data remains secure, even if an attacker gains access to a slice.

7.2.3. Lifecycle Security

The DSIF framework provides security across all phases of the slice lifecycle:

- **Deployment Phase**: Templates are validated using cryptographic signatures to prevent tampering or injection of malicious code.
- **Activation Phase**: Role-based access controls (RBAC) are implemented to ensure that only authorized entities can modify or activate slices.
- **Operational Phase**: Continuous monitoring and real-time alerts are enabled for detecting and responding to threats.
- **Decommissioning Phase**: Residual data is securely deleted using cryptographic erasure techniques to prevent reuse or exploitation.

7.2.4. Integration of AI and Machine Learning

AI algorithms are employed to predict potential threats based on historical attack data. For instance, if a slice handling IoT healthcare device shows anomalous data usage, the system can pre-emptively isolate the slice and investigate further.

8. Expected Impact on IoT Security

Table 1 The proposed DSIF framework significantly enhances IoT security by addressing the inherent vulnerabilities of 5G network slicing

S/N	Impact	Description
1.	Improved Isolation	The framework ensures strict separation of slices, mitigating the risk of cross-slice attacks and resource leaks.
2	Enhanced Threat Detection	AI-driven threat detection minimizes response times, allowing operators to neutralize threats before they impact IoT applications.
3	Increased Resilience	The use of micro-segmentation and adaptive resource allocation ensures that even if one segment is compromised, the overall system remains operational.
4	Data Integrity and Confidentiality	End-to-end encryption and secure API protocols safeguard sensitive IoT data from interception and tampering.
5	Scalability and Flexibility	The framework adapts to the dynamic needs of IoT applications, supporting rapid deployment of new slices without compromising security.

Below is a conceptual diagram of the Dynamic Secure Isolation Framework (DSIF)

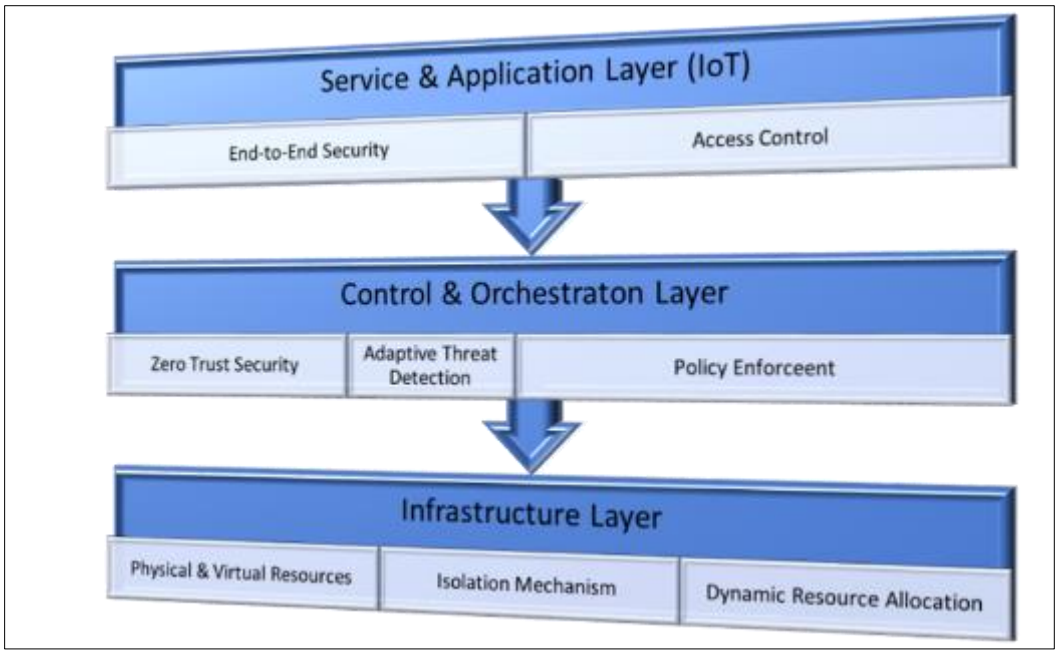

Figure 2 Dynamic Secure Isolation Framework (DSIF)

The Dynamic Secure Isolation Framework (DSIF) overcomes the limitations of existing frameworks by integrating advanced technologies like AI-driven threat detection, Zero Trust principles, and dynamic resource management. Its multi-layered architecture ensures robust isolation, secure lifecycle management, and proactive threat mitigation, making it an ideal solution for securing 5G network slicing in IoT environments. By addressing vulnerabilities across all phases of the slice lifecycle and enhancing operational resilience, DSIF sets a new benchmark for securing the future of IoT in 5G networks.

9. Discussion

The telecom sector is undergoing an important shift due to the flexible potential of 5G network slicing, particularly in relation to IoT applications. However, secure slicing has certain disadvantages that should be carefully examined, just like any revolutionary breakthrough. Furthermore, the development of cutting-edge technologies such as AI-driven security monitoring holds great potential for overcoming these problems and improving the security of 5G networks.

9.1. Challenges of Secure Slicing

9.1.1. Cost of Implementation

One of the most major challenges to achieving secure slicing is the high expense involved with its deployment and management. Implementing technologies like SDN and NFV involves large upfront expenditures in infrastructure upgrades, including virtualization systems, centralized control systems, and monitoring tools. The cost of maintaining strong isolation measures, such as micro-segmentation and sophisticated encryption, significantly raises operating costs for telecom providers. Furthermore, preserving the security of slices necessitates frequent upgrades, ongoing monitoring, and the implementation of mitigation systems all of which call for highly qualified staff and advanced equipment. These expenses may be especially unaffordable for smaller companies or areas with less advanced technology.

9.1.2. Latency Concerns

Latency is a critical component in 5G-enabled IoT, especially for applications like autonomous vehicles, telemedicine, and industrial automation that demand ultra-reliable low-latency communication (URLLC). Secure slicing introduces added layers of encryption, authentication, and traffic monitoring, which can increase processing time. AI-based anomaly detection systems and encryption protocols may slow down traffic flows, potentially compromising the performance of latency-sensitive applications. Striking a balance between robust security measures and low-latency requirements remains a major challenge in network slicing.

9.1.3. Complexity in Lifecycle Management

Managing the entire lifecycle of network slices, from deployment to decommissioning, is highly complex. Each phase introduces vulnerabilities that necessitate customized security solutions. Thus, the dynamic nature of slice activating and scaling increases the likelihood of misconfigurations, which attackers can exploit. Additionally, ensuring robust security for inter-slice and intra-slice communication adds another layer of complication. The necessity for continuous integration and real-time upgrades to address emerging threats makes lifecycle management a resource-intensive and sophisticated procedure.

9.1.4. Scalability and Resource Allocation

There is a persistent problem with the scalability of secure slicing, particularly in large-scale IoT environments, where the need for more slices rises with the number of devices and applications. Each slice needs to be sufficiently isolated and secured, which necessitates a corresponding increase in resources, which can put a strain on network capacity and infrastructure, particularly during periods of high usage. Operators must balance resource allocation between slices without sacrificing security or performance, which calls for sophisticated traffic prediction and management systems.

9.1.5. Evolving Threat Landscape

Another level of difficulty is added by the changing nature of cyber threats. Attackers are always coming up with new ways to take advantage of gaps in management systems, communication routes, and APIs. As slices are inherently dynamic, securing them against threats like denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, and data breaches requires adaptive and proactive solutions.

9.2. Emerging Technologies for Enhancing Secure Slicing

Despite the challenges, emerging technologies offer promising solutions to enhance the security of 5G network slicing. Among these, AI-driven security monitoring stands out as a game-changer.

9.2.1. AI-Driven Security Monitoring

Through the development of proactive and adaptable monitoring systems, artificial intelligence (AI) and machine learning (ML) are revolutionizing the security landscape. AI-powered security solutions are more accurate than conventional systems at spotting irregularities and possible threats because they can evaluate enormous volumes of data in real time. Artificial intelligence algorithms, for instance, are able to identify anomalous traffic patterns that may be a sign of a DoS attack or illegal access attempts in slices. AI can also predict possible vulnerabilities using predictive analytics, which is based on past data and present trends. This allows operators to take precautions before threats become real.

AI's ability to automate security tasks, such as anomaly detection, threat mitigation, and resource allocation, significantly reduces the operational burden on human administrators. This is particularly valuable in managing the complexity of secure slicing, as AI systems can dynamically reconfigure slices, isolate compromised segments, and optimize resource utilization without manual intervention.

9.2.2. Blockchain for Secure Communication

Blockchain technology is emerging as a potential solution for enhancing inter-slice and intra-slice communication. Through the provision of a decentralized and tamper-proof ledger, blockchain ensures data integrity and prevents unauthorized modifications during communication. It can also be used to authenticate devices and users in IoT environments, further strengthening the security of slices.

9.2.3. Quantum Cryptography

As traditional encryption methods face limitations in protecting against advanced attacks, quantum cryptography offers a new layer of security. Leveraging the principles of quantum mechanics, this technology ensures that any attempt to intercept or tamper with encrypted data is immediately detectable. While still in its infancy, quantum cryptography holds significant promise for securing 5G network slices against future threats.

9.2.4. Dynamic Isolation Techniques

Advances in dynamic isolation techniques, such as micro-segmentation and context-aware access controls, are further enhancing slice security. These methods enable real-time adjustments to isolation levels based on the sensitivity of applications and the current threat landscape. For instance, slices handling critical IoT applications, like healthcare or

industrial automation, can be dynamically assigned stricter isolation policies during periods of heightened threat activity.

9.2.5. Zero Trust Architecture (ZTA)

The adoption of ZTA principles in network slicing ensures that no user, device, or application is inherently trusted. Every interaction within the network requires authentication and authorization, reducing the risk of insider threats and unauthorized access. ZTA complements AI-driven monitoring by enforcing strict access controls and verifying the identity of every entity interacting with slices.

Despite the immense scope of developing technologies, caution must be used when integrating them with network slicing. Cost and complexity continue to be major obstacles to these technologies' broad use. Prioritizing the solutions that provide the optimum balance between operational viability and security enhancement is imperative for operators. In order to create standardized standards and best practices for secure slicing, cooperation between industry stakeholders, academic institutions, and regulatory agencies is also crucial.

10. Conclusion

The flexibility and efficiency of network slicing have enabled the emergence of 5G-enabled IoT, which has opened revolutionary possibilities across industries. For IoT services to remain available, secure, and confidential, secure separation between slices is essential. The suggested Dynamic Secure Isolation Framework (DSIF), which addresses vulnerabilities throughout the slicing lifecycle and makes use of technologies like Software-Defined Networking (SDN), Network Function Virtualization (NFV), and AI-driven security monitoring, provides a strong way to reduce threats. This framework guarantees the scalability and robustness required for the ever-changing demands of IoT applications, in addition to improving security.

To fully utilize the potential of secured slicing, stakeholders must embrace cutting-edge technologies like blockchain and quantum cryptography and give top priority to implementing proactive security measures like dynamic isolation approaches and Zero Trust Architecture (ZTA). Researchers, business executives and regulators must work together to create the best practices and frameworks that ensure secure and efficient network slicing in 5G-enabled IoT environments. Insights from other industries, such as oil and gas, demonstrate the value of structured approaches like stakeholder collaboration, process optimization, and advanced technology integration [38]. Adapting these methodologies can provide a robust foundation for achieving operational efficiency, regulatory compliance, and security in complex systems like 5G networks. Future studies should concentrate on improving AI-powered threat detection, investigating affordable isolation techniques, and promoting the real-world use of quantum-secure technologies. The next generation of IoT-driven technologies will have a safe and expandable base thanks to these combined efforts.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Nuriev, M., Kalyashina, A., Smirnov, Y., Gumerova, G., and Gadzhieva, G. "The 5g revolution transforming connectivity and powering innovations", E3S Web of Conferences, 2024, 515:04008. Available from https://doi.org/10.1051/e3sconf/202451504008

[2] Pawar, S., Bommisetty, L., & Venkatesh, T. G. A high capacity preamble sequence for random access in 5g iot networks: design and analysis. International Journal of Wireless Information Networks. 2022. Available from https://doi.org/10.1007/s10776-022-00587-2

[3] Kenner, A., and Oladele, O. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) in Telecommunication: A Computer Science Perspective.2024.

[4] Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., Sousa, X. R., & Serôdio, C.. Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. Future Internet, 2024; 16(7), 226. Available from https://doi.org/10.3390/fi16070226

[5] Singh, V. P., Singh, M. P., Hegde, S., & Gupta, M. Security in 5G Network Slices: Concerns and Opportunities. IEEE Access. 2024. Available from https://doi.org/10.1109/ACCESS.2024.3386632

[6] Mansour, M., Gamal, A., Ahmed, A. I., Said, L. A., Elbaz, A., Herencsar, N., & Soltan, A. Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. Energies. 2023; 16(8), 3465. Available from https://doi.org/10.3390/en16083465

[7] Ezigbo, L., Okoye, F., & Chibueze, K. Advancements and Challenges in 5G Network Slicing: A Comprehensive Review. International Conference Of Engineering Innovation For Sustainable Development (ICEISD). 2024

[8] Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. Computer Networks, 2019,167, 106984. Available from https://doi.org/10.1016/j.comnet.2019.106984

[9] Gao, S., Lin, R., Fu, Y., Li, H., & Cao, J. Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey. Electronics. 2024; 13(10), 1860. Available from https://doi.org/10.3390/electronics13101860

[10] Kaur, R., Gabrijelčič, D., & Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023; 97, 101804. Available from https://doi.org/10.1016/j.inffus.2023.101804

[11] Lorincz, J., Kukuruzović, A., & Blažević, Z. A Comprehensive Overview of Network Slicing for Improving the Energy Efficiency of Fifth-Generation Networks. Sensors. 2024; 24(10), 3242. Available from https://doi.org/10.3390/s24103242

[12] Qureshi, H. N., Manalastas, M., Ijaz, A., Imran, A., Liu, Y., & Al Kalaa, M. O. Communication Requirements in 5G-Enabled Healthcare Applications: Review and Considerations. Healthcare. 2022; 10(2), 293. Available from https://doi.org/10.3390/healthcare10020293

[13] Walia, J. S., Hämmäinen, H., Kilkki, K., & Yrjölä, S. 5G network slicing strategies for a smart factory. Computers in Industry. 2019; 111, 108–120. Available from https://doi.org/10.1016/j.compind.2019.07.006

[14] Botez, R., Pasca, A. -G., Sferle, A. -T., Ivanciu, I. -A., & Dobrota, V. Efficient Network Slicing with SDN and Heuristic Algorithm for Low Latency Services in 5G/B5G Networks. Sensors. 2023; 23(13), 6053. Available from https://doi.org/10.3390/s23136053

[15] Khadmaoui-Bichouna, M., Escolar, A.M., Alcaraz-Calero, J.M., et al. Design and implementation of an integrated OWC and RF network slicing-based architecture over hybrid LiFi and 5G networks. Wireless Networks 2024. Available from https://doi.org/10.1007/s11276-024-03848-5

[16] Yadav, R., Kamran, R., Jha, P., & Karandikar, A. An architecture for control plane slicing in beyond 5G networks. Computer Networks. 2024; 249, 110511. Available from https://doi.org/10.1016/j.comnet.2024.110511

[17] Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., Soos, G., Ficzere, D., Maliosz, M., & Toka, L. 5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps. Sensors. 2020; 20(3), 828. Available from https://doi.org/10.3390/s20030828

[18] Pons, M., Valenzuela, E., Rodríguez, B., Nolazco-Flores, J. A., & Del-Valle-Soto, C. Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review. Sensors. 2023; 23(8), 3876. Available from https://doi.org/10.3390/s23083876

[19] Khan, B., Jangsher, S., Ahmed, A., and Al-Dweik, A. URLLC and eMBB in 5G Industrial IoT: A Survey. 2022; Available from https://doi.org/10.36227/techrxiv.19106795

[20] Alnaim, A.K. Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security. Int. J. Inf. Secur. 2024; 23, 3569–3589. Available from https://doi.org/10.1007/s10207-024-00900-5

[21] Li, X., Ni, R., Chen, J., Lyu, Y., Rong, Z., and Du, R. End-to-End Network Slicing in Radio Access Network, Transport Network and Core Network Domains. IEEE Access. 2020; 8. Available from https://doi.org/10.1109/ACCESS.2020.2972105.

[22] Subedi, P., Alsadoon, A., Prasad, P.W.C. et al. Network slicing: a next generation 5G perspective. J Wireless Com Network, 2021; 102. Available from https://doi.org/10.1186/s13638-021-01983-7

[23] Yamini, K. .Network Slicing in 5G Systems: Challenges, Opportunities and Implementation Approaches. International Journal of Innovative Research in Information Security. 2024; 10(2):51–56. Available from doi: https://doi.org/10.26562/ijiris.2023.v1002.02

[24] Olimid, R. F., and Nencioni, G. 5G Network Slicing: A Security Overview. *IEEE Access*. 2020; Available from https://doi.org/10.1109/ACCESS.2020.2997702

[25] Alwakeel, A. M., and Alnaim, A. K. Network Slicing in 6G: A Strategic Framework for IoT in Smart Cities. Sensors. 2024; 24(13), 4254. Available from https://doi.org/10.3390/s24134254

[26] Lee, P. and Lin, F. Tackling IoT Scalability with 5G NFV-Enabled Network Slicing. Advances in Internet of Things. 2021; 11, 123-139. Available from https://doi.org/10.4236/ait.2021.113009

[27] Siddiqi, M. A., Yu, H., and Joung, J. 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices. Electronics. 2019; 8(9), 981. Available from https://doi.org/10.3390/electronics8090981

[28] Lin, J. Y., Chou, P. H., and Hwang, R. H. Dynamic Resource Allocation for Network Slicing with Multi-Tenants in 5G Two-Tier Networks. Sensors. 2023; 23(10), 4698. Available from https://doi.org/10.3390/s23104698

[29] Suganya, D., and Santhosh Babu, A. V. Investigation Study on Secured Data Transmission in 5G Networks with Internet of Things. *International Journal of Scientific & Technology Research*. 2020 9(6), 1123-1129.

[30] Abood, M. J., and Abdul-Majeed, G. H. Classification of network slicing threats based on slicing enablers: A survey. International Journal of Intelligent Networks. 2023; 4, 103–112. Available from https://doi.org/10.1016/j.ijin.2023.04.002

[31] Stephen, A., Vijayalakshmi, A., Broody, J., Sathishkumar, J., Abishek, E., and Sathish, P. Detection of Man in The Middle Attack in 5G IOT using Machine Learning. 2023. Available from https://doi.org/10.1109/ICRASET59632.2023.10420166

[32] Chiti, F., Morosi, S., and Bartoli, C. An Integrated Software-Defined Networking–Network Function Virtualization Architecture for 5G RAN–Multi-Access Edge Computing Slice Management in the Internet of Industrial Things. Computers. 2024; 13(9), 226. Available from https://doi.org/10.3390/computers13090226

[33] Park, K., Sung, S., Kim, H., and Jung, J. Technology trends and challenges in SDN and service assurance for end-to-end network slicing. Computer Networks. 2023; 234, 109908. Available from https://doi.org/10.1016/j.comnet.2023.109908

[34] Esmaeily, A., and Kralevska, K. Orchestrating Isolated Network Slices in 5G Networks. Electronics. 2024; 13(8), 1548. Available from https://doi.org/10.3390/electronics13081548

[35] Wong, S., Han, B., and Schotten, H. D. 5G Network Slice Isolation. Network. 2022; 2(1), 153-167. Available from https://doi.org/10.3390/network2010011

[36] Knapp, E. D., & Langill, J. T. Industrial Network Design and Architecture. In Elsevier eBooks (pp. 85–120). 2014. Available from https://doi.org/10.1016/b978-0-12-420114-9.00005-8

[37] Dogani, J., Namvar, R., and Khunjush, F. Auto-scaling techniques in container-based cloud and edge/fog computing: Taxonomy and survey. Computer Communications. 2023. 209, 120–150. https://doi.org/10.1016/j.comcom.2023.06.010

[38] Bello A, Magi F, Abaneme O, Achumba U, OBALALU A, Fakeyede M. Using Business Analysis to Enhance Sustainability and Environmental Compliance in Oil and Gas: A Strategic Framework for Reducing Carbon Footprint. 2024 Nov, 10(50):76-5. https://itegam-jetia.org/journal/index.php/jetia/article/view/1303