Enhancing 5G Infrastructure to Withstand Emerging Digital Threats

Andreea BENCHEA
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
andreea.benchea@stud.etti.upb.ro

Abstract

The advent and rapid expansion of 5G technology brings substantial advancements in communication capabilities, characterized by ultra-low latency, enhanced bandwidth, and massive device connectivity. However, this technological evolution simultaneously exposes critical infrastructure to a broad spectrum of sophisticated and evolving digital threats. This paper addresses the security challenges inherent to 5G networks and proposes a set of advanced, intelligent solutions tailored to their architectural complexity. The proposed measures include Zero Trust Architecture (ZTA), artificial intelligence-based behavioral analytics, federated learning, blockchain-enabled device authentication, and secure orchestration of network slicing. These methodologies offer a scalable, proactive, and privacy-conscious security framework capable of ensuring operational resilience and data integrity. The objective of this work is to emphasize the necessity of adopting adaptive and future-ready defense mechanisms to safeguard the robustness and reliability of 5G infrastructures against emerging cyber threats.

Index terms: 5G security, Artificial Intelligence, cyber threats, network slicing, Zero Trust Architecture

1. Introduction

Fifth-generation mobile networks represent a pivotal step in the evolution of global telecommunications infrastructure, offering capabilities that significantly surpass those of previous generations. With enhanced speed, lower latency, and the ability to support a massive number of connected devices simultaneously, 5G is poised to facilitate the growth of transformative technologies, including autonomous systems, remote surgery, real-time analytics, and large-scale smart city deployments [1].

Beyond its transformative potential, 5G introduces a paradigm shift in the architecture of communication systems. Unlike its predecessors, 5G is built upon a software-centric framework that incorporates virtualization, cloud-native infrastructure, and edge computing. These characteristics enable agility and scalability but also open the door to new classes of attacks that target dynamic network functions, orchestration layers, and APIs. This new complexity demands continuous visibility, real-time threat detection, and automated defense mechanisms.

In parallel, the vast expansion of connected devices, from personal wearables to industrial IoT endpoints, generates an explosion of data, much of it sensitive or mission-critical. In this context, ensuring data confidentiality, integrity, and availability becomes paramount. The convergence of AI, automation, and 5G network services requires security solutions that are not only robust but also

context-aware, adaptive, and aligned with privacy-preserving principles. The challenge is no longer only about preventing breaches but about architecting inherently resilient systems.

However, the widespread implementation of 5G infrastructure also brings about new and complex cybersecurity concerns. As the architecture becomes more open and distributed, new attack surfaces emerge, affecting everything from core network components to edge devices and user endpoints. Moreover, the sheer scale of interconnectivity envisioned by 5G increases the likelihood of vulnerabilities being exploited and threats propagating rapidly across systems [2].

To address these risks, the security of 5G networks must be treated as a foundational design principle rather than a peripheral consideration. Traditional, static security approaches are no longer sufficient in a hyperconnected, real-time environment. Instead, proactive and adaptive security mechanisms are required to ensure resilience, privacy, and trust in next-generation mobile networks.

2. Threat Landscape in 5G Networks

The architecture and operational complexity of 5G introduce multiple vectors for sophisticated digital threats. Below are key categories of risks identified in current 5G deployments:

- **Virtualized Network Functions (VNFs)**: The use of VNFs-software-defined equivalents of traditional network functions-poses significant challenges. VNFs may be exploited through techniques such as malware injection, insecure APIs, configuration errors, or privilege escalation attacks. They also introduce new dependencies on software supply chains, increasing systemic risk [3].
- **Edge Computing Nodes**: Edge computing decentralizes processing by relocating computational tasks closer to end users and devices. While this improves performance and reduces latency, it creates localized targets for attackers. Edge nodes often operate in less secure environments and are susceptible to data interception, spoofing, and unauthorized access [4].
- **Supply Chain Vulnerabilities**: The involvement of multiple vendors in building and maintaining 5G networks expands the attack surface via potentially insecure hardware, firmware backdoors, or compromised development processes. These vulnerabilities can be exploited to gain long-term, undetected access to core infrastructure [5].
- **Network Slicing Attacks**: 5G allows operators to create isolated logical networks (slices) tailored for different services. However, improper slice isolation or insecure orchestration may lead to data leakage, denial of service (DoS), or privilege escalation across slices [6].
- **IoT Exploitation**: 5G is expected to connect tens of billions of IoT devices. Many of these devices lack strong security configurations and are often deployed in high-risk environments. Exploiting insecure IoT endpoints, attackers can launch botnet-based DDoS attacks or pivot into critical infrastructure systems [7].

The scale, heterogeneity, and real-time nature of 5G amplify these threats, necessitating intelligent, context-aware, and proactive defense mechanisms that go beyond static firewalls and manual monitoring.

3. Advanced Security Solutions for 5G

3.1. Zero Trust Architecture (ZTA)

Zero Trust Architecture is based on the principle of "never trust, always verify." In the context of 5G, ZTA eliminates implicit trust between devices, services, and users by enforcing strict identity verification, real-time monitoring, and access control regardless of location. It is particularly relevant for microservices, virtualized network functions (VNFs), and mobile edge environments [2][3].

For example, a telecom operator could implement ZTA by requiring all components-whether in the core network or at the edge-to authenticate through a centralized identity and policy enforcement system. If a rogue base station attempts to connect to the network, the access request will be evaluated against device identity, behavior history, geolocation, and role-based permissions. If any anomaly is detected (e.g., unusual login time, inconsistent firmware signature, or unregistered IP range), access is denied, and a security alert is triggered. This prevents lateral movement by potentially compromised nodes and ensures that access is strictly limited to verified, authorized actors.

3.2. AI-Based Behavioral Analytics (UEBA)

User and Entity Behavior Analytics (UEBA) applies machine learning to establish baselines of normal behavior and detect deviations that may indicate insider threats, advanced persistent threats (APTs), or misconfigurations. In 5G networks, UEBA can be deployed across slices and virtualized components to monitor network traffic patterns and user behavior, identifying threats in near real-time and automating response actions [2][5].

As an example, consider a smart grid operator managing power distribution across multiple cities via a dedicated 5G slice. Under typical conditions, devices follow consistent communication schedules and interact with known control centers. If a UEBA system detects that one sensor node suddenly initiates large volumes of outbound connections to foreign IP addresses during off-peak hours, it flags the event as anomalous. The platform then isolates the device, alerts administrators, and initiates a forensic analysis to determine whether the device has been compromised or misconfigured.

3.3. Federated Learning (FL)

Federated learning enables AI models to be trained across multiple edge devices without the need to share raw data with a central server, thus preserving user privacy and reducing communication overhead. In 5G, where edge computing is prominent, FL allows distributed threat detection and adaptive security intelligence while keeping sensitive data localized [4].

A practical example might involve multiple hospitals using connected medical devices such as infusion pumps, monitors, or diagnostic equipment. Rather than uploading patient data to the cloud, which could expose sensitive health information, each device uses its local data to improve a machine learning model that detects device malfunctions or security anomalies. The model updates (not the data) are sent to a central aggregator, which merges them into a global model and sends it back to all devices. This allows the network to learn from localized incidents (e.g., attempted ransomware injections on a single device) and preempt similar attacks elsewhere, without breaching patient confidentiality.

3.4. Blockchain for Device Authentication and Integrity

Blockchain technology provides a tamper-proof mechanism for tracking authentication events and securing device identities. In 5G infrastructures, blockchain can be applied to validate software updates, authenticate connected devices, and maintain secure records of configuration changes. This enhances transparency and accountability while mitigating risks associated with spoofing and unauthorized access [5][7].

For instance, a mobile operator may maintain a private blockchain ledger where every network device, from base stations to IoT sensors, must register and verify its identity. When a firmware update is issued, the cryptographic hash of the update package is recorded on the blockchain. Devices downloading the update validate it against the hash. If a malicious actor attempts to introduce a tampered update (e.g., with embedded spyware), the hash mismatch alerts the blockchain node, and the update is rejected. This decentralized trust mechanism ensures end-to-end integrity across highly distributed 5G ecosystems.

3.5. Secure Network Slicing Orchestration

Network slicing enables operators to allocate isolated virtual networks to support diverse applications. However, without secure orchestration, vulnerabilities in one slice could compromise others. AI-powered orchestration platforms can dynamically enforce access controls, monitor performance, and isolate threats within individual slices. According to 3GPP specifications, strong authentication, integrity protection, and isolation are essential to prevent cross-slice exploits [6].

For example, consider a telecom provider offering separate network slices to autonomous vehicle fleets, public safety services, and streaming media. If the orchestration system detects that traffic in the vehicle fleet slice suddenly spikes with patterns resembling a DDoS attack, it automatically reroutes critical telemetry to backup slices, applies stricter firewall rules, and temporarily isolates the impacted slice. Meanwhile, other services continue operating without degradation. This segmentation ensures that malicious activity in one slice does not cascade into other mission-critical services, maintaining overall network reliability and trust.

4. Regulatory, Ethical and Operational Considerations

Securing 5G infrastructure is not solely a technical challenge, it requires alignment with legal frameworks, ethical guidelines, and operational strategies that span national and international domains. At the regulatory level, one of the key instruments in the European Union is the EU Toolbox for 5G Security, which outlines a coordinated set of risk mitigation measures for member states, addressing aspects such as supply chain control, access restriction, and secure software lifecycle management [5]. Complementarily, the NIS2 Directive expands the cybersecurity obligations for essential and important entities, including telecom operators, by imposing stricter incident reporting, risk assessment, and supply chain security requirements [8].

Globally, frameworks from organizations such as ITU, 3GPP, and ENISA advocate for secure-by-design principles, network resilience, and proactive threat management. These align with the growing emphasis on adopting Zero Trust principles and multi-layered defense architectures.

From an ethical standpoint, the implementation of AI-based systems within 5G security raises important concerns. Key issues include:

- Data privacy: Algorithms such as UEBA and federated learning require access to potentially sensitive metadata. Compliance with GDPR and similar data protection regulations is essential.
- Algorithmic bias: AI models trained on unbalanced or incomplete datasets may lead to biased threat assessments or unjustified access denials.
- Transparency and accountability: The use of opaque decision-making processes must be countered by explainable AI (XAI) methods and clear human oversight protocols.

Operationally, integrating the aforementioned solutions into real-world 5G networks demands a significant upgrade in infrastructure, processes, and human competencies. Network operators must:

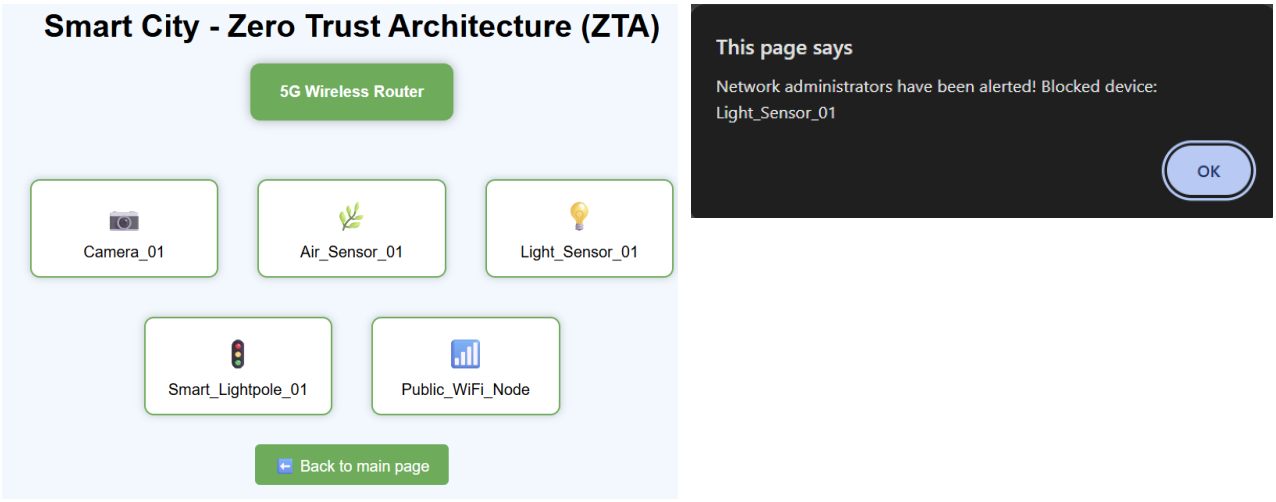
- Invest in automation and orchestration platforms capable of responding to threats in real-time.
- Establish inter-industry and public-private collaboration frameworks to share threat intelligence and mitigation strategies.
- Train personnel in AI operations (AIOps), blockchain governance, and Zero Trust deployment models.

A robust 5G security posture thus requires a convergence of technical excellence, ethical diligence, and regulatory compliance.

5. Case study - Applying 5G security solutions in a smart city scenario

This study presents the practical deployment of 5G security strategies within a simulated smart city infrastructure. The developed model connects critical systems including public transportation, traffic signaling, video surveillance, environmental monitoring sensors, and emergency response units via a 5G network.

Fig. 1. Overview of 5G Security Strategies Implemented in the Smart City Architecture



(a) (b)

Fig. 2. (a) Device authentication interface; (b) Security alert triggered after device blocking

The initial stage involved the implementation of a Zero Trust Architecture (ZTA) across all connected assets. Each network component, such as surveillance cameras and connected streetlights, is required to verify its identity prior to accessing the infrastructure. Unauthorized devices are systematically denied access, and lateral communication between assets is permitted solely under predefined and encrypted policies, thereby significantly mitigating internal threat propagation. Within the associated simulation, network access is conditioned by password verification. Devices failing authentication after three attempts are visually blocked, and a network alert is triggered, emphasizing proactive internal security measures.

Subsequently, AI-based behavioral analytics were integrated both at the network core and edge levels to establish normative activity baselines. These systems continuously monitor real-time device interactions, detecting deviations from expected behavior. For example, if a waste sensor transmits data during unusual hours or towards unauthorized endpoints, an alert is generated and the device may be isolated for further investigation. In the simulation, real-time charts are displayed for smart sensors. Data points exceeding defined thresholds are automatically highlighted in red, facilitating the immediate detection of anomalies.

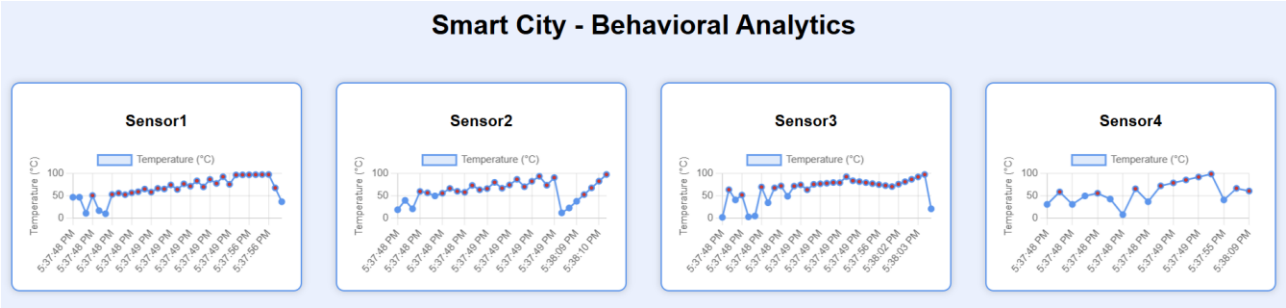
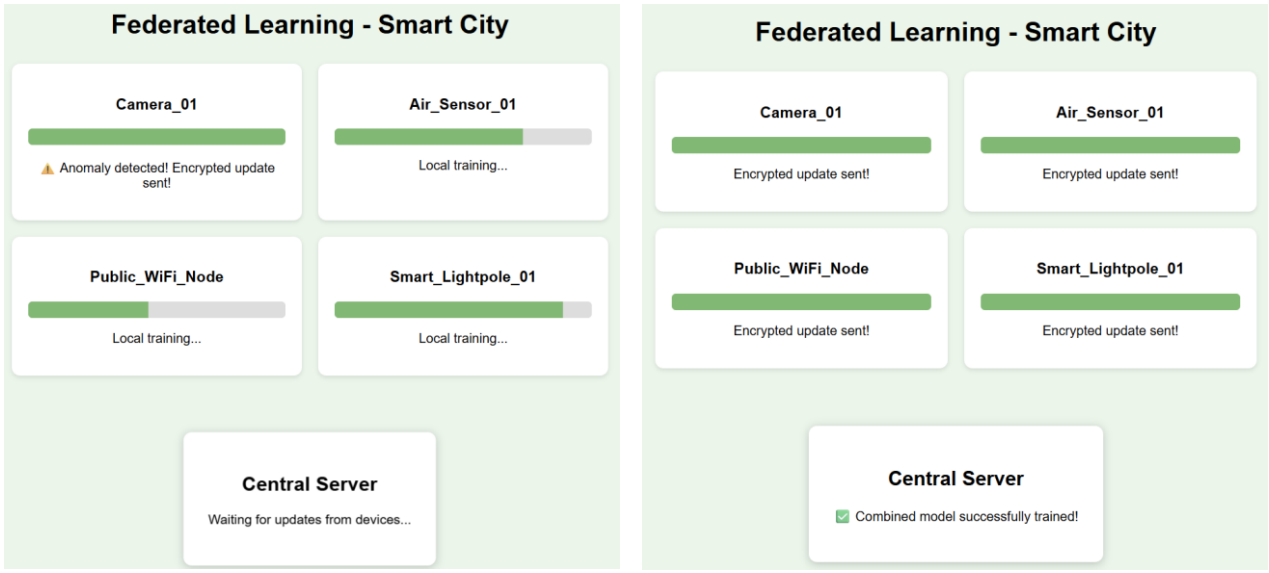


Fig. 3. Real-Time Behavioral Analytics Monitoring for Smart City Sensors

In order to enhance localized threat intelligence without compromising user privacy, Federated Learning methodologies were employed. Smart meters and environmental monitoring units train machine learning models locally and transmit solely encrypted model updates to a central aggregation node, thus maintaining data sovereignty. In the corresponding simulation, devices illustrate the local model training process and securely transmit encrypted updates. This approach ensures private data remains on the device while contributing to an improved global model.



(a) (b)

Fig. 4. (a) Local training phase with anomaly detection; (b) Successful encrypted updates and combined model training at the central server

To preserve the authenticity and integrity of devices and software updates, a blockchain-based authentication system was integrated. This immutable ledger maintains records of device registrations, configuration changes, and software update histories. Prior to the application of any update, devices verify the corresponding hash against the blockchain to prevent tampering or unauthorized modifications. Within the simulation, update hashes are validated against existing blockchain records. Updates matching the recorded hash are successfully applied, while those failing verification are promptly rejected.

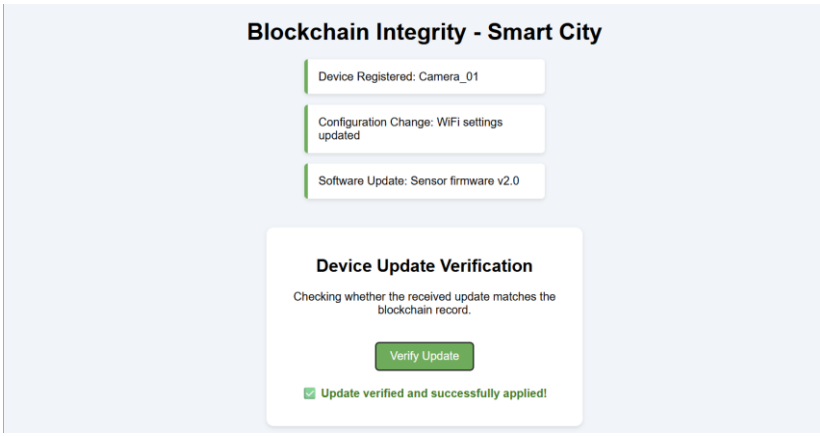


Fig. 5. Blockchain-Based Device Update Verification

In order to optimize service delivery and security, secure network slicing was employed to segment network services according to function, specifically public connectivity, emergency response, utilities, and traffic management. Each slice operates independently under the supervision of AI-based orchestration platforms, which manage resource allocation and enforce security policies. In the event of a cyberattack affecting one slice (such as a denial-of-service attack on public Wi-Fi), the remaining slices continue to operate normally, ensuring service continuity without cross-contamination. In the simulation, random attack events can be simulated, visually isolating the affected slice while maintaining normal operations across unaffected slices, thus demonstrating the resilience of a segmented network architecture.

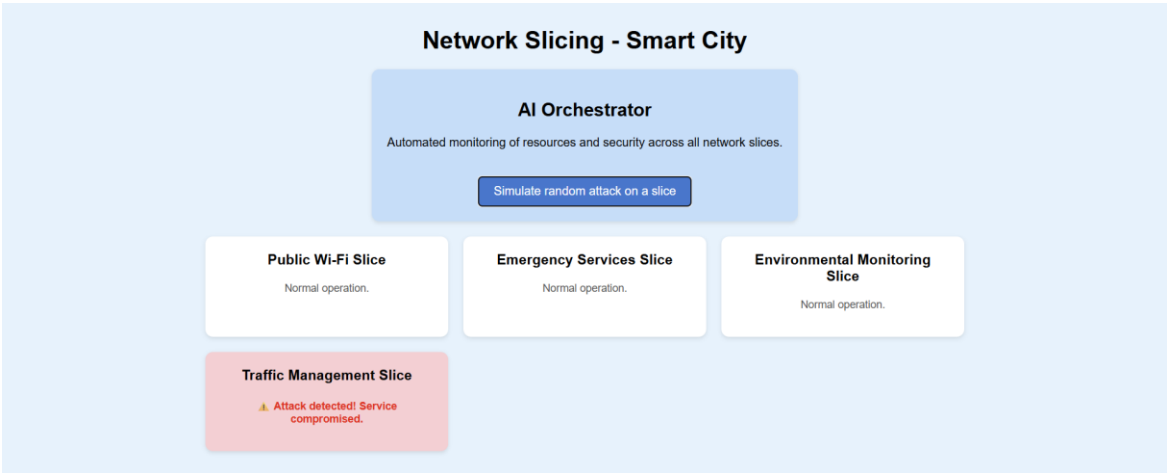


Fig. 6. Simulation of Attack Detection and Isolation in Smart City Network Slicing

6. Conclusions and future directions

The evolution of 5G networks marks a transformative milestone in modern communications, enabling capabilities such as ultra-reliable low-latency communication, massive machine-type communication, and enhanced mobile broadband. However, with these advancements come unprecedented cybersecurity risks due to the network's decentralized architecture, software-defined components, and hyper-connectivity.

This paper has examined the unique threat vectors introduced by 5G technologies and outlined a comprehensive portfolio of security mechanisms - including Zero Trust Architecture, behavioral analytics, federated learning, blockchain-based integrity verification, and secure network slicing - that collectively support a robust, adaptive, and proactive security posture.

As technology adoption accelerates, it is imperative to continue evolving these frameworks. Future efforts must prioritize:

- Developing explainable and auditable AI models that ensure transparency and traceability in automated threat detection.
- Standardizing and regulating blockchain implementations tailored to telecom requirements, ensuring they align with global interoperability and data governance policies.
- Securing the AI development lifecycle, particularly against poisoning and adversarial inputs at the edge.
- Fostering international cooperation, including harmonized cybersecurity standards, collaborative incident response protocols, and cross-border threat intelligence sharing.

The long-term security of 5G infrastructures necessitates sustained investment in specialized education, continuous workforce development, and the dynamic adaptation of regulatory frameworks to technological advancements. Safeguarding these networks constitutes an ongoing endeavor, requiring unwavering technological vigilance, operational resilience, and a firm commitment to ethical governance across all layers of the digital ecosystem.

References

[1]. International Telecommunication Union (ITU), *IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond*, Recommendation ITU-R M.2083-0, Sep. 2015. [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I%21%21PDF-E.pdf.

[2]. European Union Agency for Cybersecurity (ENISA), *Threat Landscape for 5G Networks*, Nov. 2020. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20threat%20landscape%20for%205G%20Networks.pdf.

[3]. 5GPPP, Security *Landscape - Phase 1 White Paper*, Jun. 2017. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf.

[4]. European Telecommunications Standards Institute (ETSI), *Multi-access Edge Computing (MEC); Framework and Reference Architecture*, ETSI GS MEC 003 V2.1.1, Jan. 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.01.01_60/gs_MEC003v020101p.pdf.

[5]. European Commission, *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*, Jan. 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[6]. 3GPP, *TR 33.891 - Study on security aspects of network slicing in 5G networks*, Release 15, Dec. 2018. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3358.

[7]. Symantec, *Internet Security Threat Report*, Vol. 24, Feb. 2019. [Online]. Available: https://docs.broadcom.com/doc/istr-24-2019-en.

[8]. European Union, *Directive (EU) 2022/2555 (NIS2)*, Official Journal of the European Union, Dec. 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32022L2555.