International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 11 | Nov 2025 www.irjet.net p-ISSN: 2395-0072

Security Challenges and Solutions in 5G Network Slicing

ANAND R

MSc Computer Science Student, St. Thomas (Autonomous) College, Thrissur 680001, Kerala, India

---

Abstract - *5G network slicing enables the creation of multiple virtualized network segments over a common physical infrastructure, providing tailored services for diverse applications such as enhanced mobile broadband, ultra-reliable low-latency communication, and massive IoT. While this architecture offers flexibility and efficient resource utilization, it also introduces significant security concerns. Key issues include inadequate slice isolation, vulnerabilities in inter-slice communication, dynamic resource management risks, and new attack surfaces in multi-tenant environments. Traditional security measures are insufficient to handle the dynamic and software-driven nature of 5G slices, necessitating adaptive and intelligent security frameworks. Emerging solutions leverage Machine Learning (ML) and Artificial Intelligence (AI) for real-time anomaly detection and predictive threat mitigation. Blockchain-based approaches enhance decentralized trust, secure authentication, and auditability in slice orchestration. Additionally, zero-trust architectures and automated policy enforcement ensure continuous monitoring and access control across the slice lifecycle. Future advancements will focus on scalable, intelligent, and interoperable security mechanisms, including standardized protocols, edge security integration, and quantum-resistant encryption. By combining ML-driven threat detection, blockchain trust management, and robust isolation, 5G networks can achieve resilient and secure network slicing to fully realize their potential*.

Key Words: **5G Network Slicing, Security Challenges, Machine Learning, Blockchain**

1. INTRODUCTION

The fifth generation of mobile networks (5G) represents a major technological leap in the field of wireless communication, enabling high-speed connectivity, ultra-low latency, and support for massive Internet of Things (IoT) deployments. One of the most transformative features of 5G is network slicing, which allows the creation of multiple, virtualized, and independent network segments over a shared physical infrastructure. Each slice can be tailored to meet the performance and reliability requirements of diverse services, such as enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine-type communications (mMTC). By efficiently allocating network resources, network slicing enables operators to serve multiple industries and use cases on a single 5G infrastructure. However, while this paradigm unlocks significant opportunities, it also introduces new security challenges that must be addressed to ensure reliable and secure operations.

The literature extensively discusses these challenges and highlights the growing importance of security in network slicing. The paper "Security in 5G Network Slices: Concerns and Opportunities" provides a foundational perspective on how the virtualization and multi-tenancy inherent in network slicing introduce risks such as inadequate slice isolation, misconfigurations, and vulnerabilities in inter-slice communication. As slices share the same underlying infrastructure, a breach in one slice could potentially impact other slices if isolation mechanisms fail. Similarly, dynamic resource allocation and automated slice lifecycle management can create new attack surfaces, including unauthorized access and malicious resource exploitation.

Complementing this perspective, the work "5G Network Slicing: A Security Overview" categorizes the key threats according to the 5G architecture layers and highlights the limitations of traditional security frameworks in this highly dynamic environment. It emphasizes that the reliance on software-defined networking (SDN), network function virtualization (NFV), and automated orchestration requires adaptive, slice-specific security solutions. The paper also stresses the importance of continuous monitoring, policy enforcement, and end-to-end protection across all layers of the network.

Building on these foundational studies, the recent survey "ML-Based 5G Network Slicing Security: A Comprehensive Survey" explores modern approaches that leverage Artificial Intelligence (AI) and Machine Learning (ML) to enhance security in 5G slices. These technologies enable real-time anomaly detection, predictive threat mitigation, and automated response mechanisms. The survey also examines the use of blockchain for decentralized trust management, secure authentication, and transparent auditing of slice operations. By integrating AI and blockchain with zero-trust principles, 5G networks can achieve stronger isolation, reduced attack exposure, and proactive defense strategies.

Securing 5G network slicing involves addressing several critical issues simultaneously. First, slice isolation must be rigorously enforced to ensure that a compromise in one slice does not propagate to others. Second, dynamic resource management must be secured against misconfigurations and malicious exploitation. Third, inter-slice communication channels need protection from eavesdropping and data leakage. Traditional perimeter-based security models are insufficient in such a dynamic and virtualized environment, necessitating more intelligent and adaptive solutions.

Research suggests that AI-driven anomaly detection can identify threats in real time, while blockchain can maintain trust and accountability among multiple tenants and service providers. Additionally, implementing zero-trust architectures ensures that access control and security policies are applied continuously throughout the slice lifecycle, regardless of the network segment or user role.

Looking toward the future, securing 5G network slicing will require integrated and scalable security frameworks. As networks evolve toward 6G and beyond, the complexity of slices will increase with the rise of edge computing, massive IoT, and cross-domain service orchestration. Emerging directions include quantum-resistant encryption, standardized protocols for slice interoperability, and lightweight, AI-powered security solutions for resource-constrained devices. By adopting a holistic approach that combines machine learning, blockchain trust, and rigorous isolation mechanisms, 5G networks can realize the full potential of network slicing while ensuring robust and resilient security.

In summary, the reviewed papers collectively emphasize that the success of 5G network slicing depends on addressing its unique security challenges. Leveraging adaptive and intelligent security solutions is crucial for building trustworthy, scalable, and future-ready 5G infrastructures. This paper builds upon the insights from the existing literature to explore the concerns, opportunities, and solutions in securing 5G network slicing.

I. Literature review

The evolution of 5G networks has introduced a paradigm shift in wireless communication by integrating network slicing, which allows the creation of multiple virtualized and isolated network segments on a shared infrastructure. Network slicing is essential to meet the diverse requirements of enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine-type communications (mMTC). However, with these opportunities come significant security concerns that have been widely studied in recent literature. One of the foundational works, "Security in 5G Network Slices: Concerns and Opportunities", provides an in-depth analysis of the inherent security vulnerabilities in 5G network slicing. It identifies slice isolation as a primary concern, noting that a security breach in one slice could impact other slices if proper isolation is not enforced. The study highlights that the multi-tenant environment of 5G, combined with its reliance on virtualization, introduces additional risks such as resource mismanagement and denial-of-service (DoS) attacks. The paper also discusses dynamic resource allocation and automated slice lifecycle management as new attack surfaces. Since slices are created, modified, and deleted dynamically, any misconfiguration or malicious activity in the orchestration process could compromise the entire system. Moreover, inter-slice communication can become a vector for data leakage and eavesdropping if secure mechanisms are not in place. These findings underline the inadequacy of traditional perimeter-based security solutions in addressing the highly distributed and software-driven nature of 5G networks.

The most recent contribution, "ML-Based 5G Network Slicing Security: A Comprehensive Survey", explores the role of advanced technologies such as Machine Learning (ML) and Blockchain in enhancing 5G slice security. This survey highlights how ML algorithms can be utilized for real-time anomaly detection, intrusion detection systems (IDS), and predictive threat analysis, allowing networks to anticipate and prevent attacks before they escalate. Supervised, unsupervised, and reinforcement learning models are particularly valuable for identifying abnormal traffic patterns, detecting misconfigurations, and dynamically adjusting security policies. The study also discusses the application of blockchain for decentralized trust management in multi-tenant environments. Blockchain provides immutable records of slice orchestration activities, ensures secure authentication, and allows transparent auditing of slice operations. When combined with zero-trust principles, these technologies create a highly secure environment where no entity is trusted by default, and every access request is continuously verified. The survey also identifies challenges in deploying AI and blockchain at scale, such as computational overhead, latency constraints, and the need for lightweight security models suitable for edge and IoT devices. Nevertheless, the integration of these emerging technologies is presented as a critical step toward achieving adaptive, autonomous, and scalable slice security.

Despite these advancements, the literature reveals several open research challenges in securing 5G network slicing. Current solutions are often fragmented, focusing on specific threats rather than providing comprehensive, integrated security frameworks. Additionally, standardized protocols for slice security and interoperability across vendors remain limited. As the network ecosystem moves toward 6G, new concerns such as cross-domain slice security, quantum-safe encryption, and edge-computing integration will require innovative approaches. The reviewed papers collectively indicate that intelligent, automated, and layered security mechanisms will define the future of 5G slice protection. Research is increasingly leaning toward solutions that combine ML-driven threat detection, blockchain-enabled trust, and rigorous isolation techniques, providing a roadmap for resilient and secure network slicing. Overall, the existing body of research highlights that securing 5G network slicing is a multi-dimensional challenge involving isolation, orchestration, and real-time threat detection. Early works established the core vulnerabilities of network slicing, while subsequent studies focused on layered threat analysis and adaptive solutions. Recent surveys show that AI, ML, blockchain, and zero-trust architectures are emerging as the key enablers of next-generation slice security. However, the literature also calls for comprehensive frameworks and

global standards to address the complexity and scalability demands of 5G and beyond.

1. Network Slicing

At its core, a network slice is a logically separated, end-to-end virtual network instance that runs on top of shared physical infrastructure. Despite being virtual, each slice can be uniquely configured with its own network functions, performance levels, security protocols, and management policies. This means a single 5G infrastructure can host multiple isolated networks, each tailored to a specific service type or customer requirement. This concept is fundamentally different from previous mobile network generations, where one static infrastructure was expected to serve all use cases uniformly. In 5G, network slicing supports the idea of "network-as-a-service (NaaS)", giving service providers the ability to allocate and manage network resources dynamically. A network slice is a key innovation in 5G technology that allows multiple virtual networks to run on a shared physical infrastructure. Each slice is a logically isolated, end-to-end network customized to serve specific types of services or applications. This concept enables telecom providers to tailor network performance—such as bandwidth, latency, reliability, and security—based on the unique needs of different users or industries. For example, one network slice might be designed to support high-speed video streaming, while another is optimized for low-latency communication needed in autonomous vehicles or remote surgeries. These slices can coexist without interfering with each other, even though they use the same underlying hardware. Network slicing is made possible by two key technologies: Software Defined Networking (SDN) and Network Function Virtualization (NFV). SDN separates the control functions from the physical hardware, enabling flexible and centralized management. NFV allows network functions like firewalls or routers to run as software, eliminating the need for dedicated devices. Each network slice goes through a lifecycle that includes preparation, provisioning, operation, and termination. Throughout this process, service providers can dynamically allocate or reconfigure resources based on demand. However, while network slicing offers great benefits in flexibility and efficiency, it also introduces security challenges. Slices must be carefully isolated to prevent breaches or unauthorized access. Strong authentication, encryption, and real-time monitoring are essential for maintaining secure and reliable service. In summary, network slicing transforms how mobile networks operate by enabling customized, virtualized services on a shared platform. It is a foundational element of 5G, promising to support a wide range of industries—from entertainment and healthcare to smart cities and industrial automation—each with their own dedicated “slice” of the network.

1.1. Architectural Layers of Network Slicing

network slicing is structured into three key layers, each playing a distinct role in the creation and operation of slices:

A.ResourceLayer:

This is the foundational layer, made up of physical and virtual resources such as storage, processors, routers, switches, and wireless radio access components. It includes both hardware (like servers) and software-defined elements (like virtual machines and containers). These resources may be shared across multiple slices or dedicated to a specific slice depending on required performance and isolation.

B. Network Slice Instance Layer:

This layer represents the actual network slice instances. A network slice instance is a collection of network functions (such as firewalls, gateways, and policy controllers) arranged and configured to meet particular application needs. Each slice operates independently and may share or not share resources and infrastructure with other slices.

C. Service Instance Layer:

This is the top layer, where services and applications run. Examples include 4K video streaming (eMBB), autonomous driving (URLLC), or IoT smart metering (mMTC). Each service uses the capabilities and resources provided by its corresponding network slice.

1.2. Lifecycle of a Network Slice

The operation of a network slice is managed through its lifecycle, which includes four distinct phases:

1. Preparation: In this initial phase, the network operator defines the slice’s purpose and specifications. Slice templates are created, defining performance targets, security requirements, and functional elements. This is a planning stage and does not involve actual deployment.

2. Provisioning (Instantiation and Activation): Here, the slice is instantiated based on its template. Resources and network functions are allocated, configured, and connected. The slice becomes operational and is ready to serve end-users.

3. Operation and Management: Once active, the slice is continuously monitored for performance, security, and SLA compliance. Adjustments or scaling may be performed based on dynamic demands. Fault detection and incident handling are also part of this phase.

4. Decommissioning: After its utility has been fulfilled or upon expiration, the slice is dismantled. Resources are freed or reassigned, and sensitive data is securely wiped to prevent leakage or misuse.

1.3. Use Cases and Applications of Network Slicing

5G network slicing supports a broad array of use cases, grouped primarily into three categories by the ITU and 3GPP:

1. Enhanced Mobile Broadband (eMBB): Slices in this category support high-speed internet access, high-definition video streaming, virtual/augmented reality, and similar bandwidth-intensive applications.

2. Ultra-Reliable Low-Latency Communication (URLLC): These slices are optimized for minimal latency and high reliability. Use cases include autonomous vehicles, industrial automation, and remote healthcare (like telesurgery), where even minor delays can be catastrophic.

3. Massive Machine-Type Communication (mMTC): Designed for scenarios with high device density but low data rate requirements, such as smart cities, utility meters, and large-scale IoT deployments.

Beyond these, slices are being tailored for edge computing, private enterprise networks, emergency services, and vehicle-to-everything (V2X) communication.

1.4. Key Technologies Enabling Network Slicing

Two primary technologies make network slicing feasible in 5G:

● Software Defined Networking (SDN): SDN decouples the control plane from the data plane, allowing centralized control and dynamic programming of the network. In slicing, SDN is used to define and enforce flow rules, manage traffic routing, and isolate slices from one another.

● Network Function Virtualization (NFV): NFV replaces traditional hardware-based network functions (e.g., routers, firewalls) with software instances that can run on standard servers. It allows slices to have customizable functions tailored to the needs of a service without requiring dedicated hardware.

These technologies enable rapid deployment, scalability, and dynamic reconfiguration of slices in response to changing network conditions or customer requirements

1.5. Security Implications of Network Slicing

While network slicing enhances flexibility and efficiency, it also introduces new security vulnerabilities. Since multiple virtual networks share the same physical infrastructure, ensuring isolation becomes crucial. A breach in one slice should not affect others. The documents identify several key vulnerable areas:

● Lifecycle Phases: From poorly designed slice templates to improper decommissioning that leaks data.

● Intra-Slice Communication: Vulnerabilities within a slice can lead to unauthorized access, DoS attacks, or data tampering.

● Inter-Slice Interaction: Shared resources between slices could be exploited to leak sensitive information or manipulate traffic.

● Underlying Technologies: SDN and NFV, while powerful, can be attacked via control plane exploits, compromised VNFs, or API misuse.

● End Devices: User equipment may serve as entry points for attackers, especially if weak authentication mechanisms are in place.

To mitigate these risks, the following security practices are recommended:

● Enforce logical and physical isolation between slices.

● Adopt a Zero Trust architecture that authenticates and authorizes every interaction.

● Implement strong encryption, traffic monitoring, and behavioral anomaly detection.

● Secure APIs and management interfaces with authentication and audit logs.

1.6. Understanding the Risk Landscape

In traditional mobile networks, the entire infrastructure was generally treated as a unified system with a relatively fixed set of services. With network slicing, multiple virtual networks with different performance and security requirements coexist and operate in parallel. This multi-tenancy model increases the potential attack surface significantly. Any vulnerability in one slice could potentially be exploited to compromise others, especially if strong isolation is not enforced. Furthermore, the dynamic nature of slicing—where slices can be created, modified, or deleted on demand—makes it harder to apply traditional, static security policies.

1.6.1. Lifecycle Vulnerabilities

Security threats in network slicing can emerge during any phase of the slice lifecycle, which includes preparation, provisioning, operation, and decommissioning:

1. Preparation Phase: During this stage, slice templates are designed and security requirements are defined. Poorly designed templates or the use of outdated security models can introduce vulnerabilities even before the slice becomes active.

2. Provisioning Phase: This phase involves allocating resources and configuring the slice. Attackers could exploit weak access control mechanisms in APIs or orchestration platforms to create rogue slices or alter legitimate ones.

3. Operation Phase: Once a slice is active, it becomes a live target for threats like Denial of Service (DoS) attacks, unauthorized access, and performance degradation. Monitoring, auditing, and timely updates are essential to secure this phase.

4. Decommissioning Phase: Improper shutdown and data wipeout can lead to data leakage or unauthorized reuse of virtual resources, compromising privacy and availability.

1.6.2. Intra-Slice and Inter-Slice Threats

Security issues can also be categorized based on whether they occur within a single slice (intra-slice) or between slices (inter-slice).

● Intra-Slice Security: These threats stem from within the boundaries of a single slice. For example, an end-user device connected to a slice may be compromised and used to launch attacks from within. Similarly, services operating inside the slice, if not properly isolated, can interfere with each other, leading to resource exhaustion or data corruption.

● Inter-Slice Security: In this case, a breach in one slice could be used to gain access to others, especially if the slices share resources like compute or storage. A common attack scenario involves a malicious actor launching a side-channel attack to gather sensitive data from another slice. Resource sharing, if not properly managed, becomes a serious risk in multi-slice environments.

1.6.3. Technology-Driven Risks

Two technologies enable network slicing: Software-Defined Networking (SDN) and Network Function Virtualization (NFV). While these technologies are essential for flexibility and scalability, they come with their own security concerns.

● SDN Vulnerabilities: SDN separates the control and data planes, introducing centralized controllers that become attractive targets. A compromised SDN controller could manipulate traffic flow, disable network functions, or eavesdrop on sensitive data.

● NFV Weaknesses: Virtual Network Functions (VNFs) replace traditional hardware-based network components. However, VNFs running on shared servers can be vulnerable to hypervisor attacks, VM escape, or malicious code injection, especially if tenant separation is not strictly enforced.

2. Solutions

Based on the paper, securing 5G network slicing requires a combination of advanced technologies and strategic approaches. Key solutions include implementing strong slice isolation through NFV, SDN, and micro-segmentation, ensuring that vulnerabilities in one slice do not affect others. Inter-slice communication must be protected using encryption protocols, mutual authentication, and zero-trust frameworks to prevent unauthorized access and data leakage. Machine Learning techniques enable real-time anomaly detection and predictive threat prevention, while blockchain offers decentralized trust management, immutable logging, and automated policy enforcement through smart contracts. Together, these solutions create a layered, adaptive security framework capable of addressing the dynamic and multi-tenant nature of 5G slicing.

1.1. Slice Isolation Solutions

One of the most critical security concerns in 5G network slicing is maintaining strict slice isolation. Without proper isolation, a compromise in one slice can propagate to others, leading to cross-slice attacks and system-wide vulnerabilities. Effective solutions to this problem are based on a combination of virtualization technologies, resource allocation policies, and monitoring frameworks. Network Function Virtualization (NFV) enables the separation of network functions into independent virtual machines or containers, ensuring that the execution of one slice does not interfere with another. Using hypervisor-level isolation with hardware-assisted virtualization can further strengthen this separation. Additionally, Software-Defined Networking (SDN) controllers can enforce traffic segmentation rules, making it nearly impossible for traffic from one slice to leak into another without authorization.

From a policy perspective, dynamic resource allocation combined with access control mechanisms ensures that no slice can consume resources allocated to other slices. AI-based anomaly detection techniques, as highlighted in the ML-Based 5G Network Slicing Security survey, can identify unusual cross-slice behaviors that may indicate a breach in isolation. Blockchain technology is also emerging as a supportive mechanism, offering decentralized record-keeping to verify resource ownership and prevent unauthorized reallocation of resources. The use of micro-segmentation within each slice provides an additional layer of protection, preventing lateral movement of threats even if part of a slice is compromised. Finally, continuous runtime monitoring with automated alerts and corrective actions ensures that isolation breaches are detected and mitigated in real time. Together, these solutions create a robust framework for slice isolation, preserving the independence and security of each virtual network segment in 5G.

1.2. Inter-Slice Communication Security Solutions

Securing inter-slice communication is essential, as 5G slices often need to exchange data between applications or share network services. Vulnerabilities in this area can lead to data leakage, eavesdropping, and man-in-the-middle attacks. Solutions to secure inter-slice communication rely on encryption, authentication, and secure orchestration mechanisms. End-to-end encryption using modern cryptographic standards ensures that even if traffic is intercepted, it cannot be read or tampered with. Protocols like IPSec, TLS 1.3, and QUIC can be adapted to secure communication both within and between slices, while mutual authentication ensures that only verified slices can interact.

In addition to encryption, zero-trust security architectures play a critical role in inter-slice communication. Zero-trust principles require that every access attempt between slices is continuously validated based on identity, context, and risk level. Blockchain can further enhance trust by maintaining immutable logs of inter-slice communication events, which

can be audited in case of a security incident. Furthermore, secure APIs and slice gateways can be used to mediate communication, enforcing policy-based access control and filtering suspicious traffic. Machine Learning (ML) techniques provide an additional protective layer by monitoring inter-slice traffic patterns in real time, identifying potential anomalies that may indicate unauthorized access or lateral attacks.

To prevent exploitation via orchestration layers, secure orchestration frameworks with role-based access control and integrity checks must be implemented. Orchestration platforms should validate all inter-slice requests and enforce strict separation of data plane and control plane traffic. Regular security audits, penetration testing, and runtime verification help ensure that inter-slice communication remains resilient to attacks. By combining encryption, authentication, zero-trust principles, and intelligent monitoring, 5G networks can ensure that inter-slice communication is both secure and reliable, preventing data exposure while maintaining service efficiency.

1.3. Dynamic Resource Management and Orchestration Security Solutions

Dynamic resource allocation and automated orchestration are vital to the flexibility and scalability of 5G network slicing, but they also introduce significant security risks. Misconfigurations or unauthorized manipulations in the orchestration layer can lead to denial-of-service (DoS) attacks, resource hijacking, and slice performance degradation. Addressing these challenges requires an integrated approach combining secure orchestration frameworks, AI-driven management, and blockchain-based verification.

First, secure orchestration platforms must enforce strict access controls and authentication for all resource allocation requests. Role-based access ensures that only authorized personnel or automated systems can modify resource assignments. Integrating policy-driven automation reduces human errors that could lead to security vulnerabilities. Orchestration logs should be cryptographically signed to prevent tampering and ensure accountability. AI-based solutions are highly effective in this context, as highlighted in the ML-Based 5G Network Slicing Security paper. Machine Learning algorithms can continuously monitor resource usage and orchestration decisions, detecting anomalies that may indicate malicious activity or misconfigurations.

Blockchain technology can enhance orchestration security by providing a decentralized ledger to record all slice operations, resource allocations, and modifications. This immutable record ensures transparency and prevents rollback or unauthorized changes. Combining blockchain with smart contracts allows automated, policy-driven allocation and scaling of resources without manual intervention. Additionally, network simulation and testing in sandbox environments can identify potential orchestration vulnerabilities before deployment.

Lastly, runtime verification and continuous monitoring are essential. Integrating feedback loops into orchestration ensures that resource allocation decisions adapt to the network state while remaining secure. If an anomaly or attack is detected, the system can automatically isolate affected slices, reallocate resources, and alert administrators. By combining secure orchestration, AI-driven monitoring, and blockchain verification, 5G networks can protect dynamic resource management from exploitation while maintaining high performance and reliability.

1.4. Machine Learning-Based Security Solutions

Machine Learning (ML) has emerged as one of the most promising approaches to enhance 5G network slicing security due to its ability to handle dynamic, complex, and high-volume network environments. Traditional security mechanisms are often reactive and rule-based, which makes them insufficient for detecting sophisticated, evolving threats in real time. ML techniques, by contrast, can proactively identify anomalies, predict attacks, and support automated responses across the 5G slice lifecycle.

One key application of ML is in anomaly and intrusion detection. By continuously analyzing traffic patterns, resource usage, and slice orchestration events, ML models can identify deviations from normal behavior that may indicate malicious activity, such as denial-of-service attacks, inter-slice intrusions, or data exfiltration attempts. Unsupervised learning algorithms like clustering and autoencoders are particularly effective in detecting unknown or zero-day threats because they do not rely on predefined signatures. Supervised learning models, trained on historical attack datasets, can classify known threats quickly and accurately, while reinforcement learning techniques can dynamically adapt slice security policies based on changing network conditions.

Another significant contribution of ML lies in predictive threat mitigation. Models can forecast potential security risks, such as slice resource exhaustion or orchestration misconfigurations, and trigger preventive actions before an attack escalates. Integration with zero-trust architectures enables ML systems to continuously validate user and device behaviors, flagging suspicious activities in real time. Moreover, combining ML with blockchain technology enhances trust and transparency in slice operations; for example, ML can detect abnormal access requests, and blockchain can record and verify them for auditability.

ML also supports orchestration and resource management security by analyzing slice demands, detecting anomalies in allocation, and automatically reallocating resources if a security breach is suspected. However, challenges remain, including the computational overhead of real-time ML inference and the need for lightweight models for edge and IoT devices. Nevertheless, integrating ML-based solutions into 5G network slicing provides a robust, scalable, and adaptive framework for threat detection, prediction, and

automated response, significantly improving the overall security posture of next-generation mobile networks.

1.5. Blockchain and Zero-Trust Security Solutions

Blockchain and Zero-Trust architectures are increasingly recognized as essential components for securing 5G network slicing due to their ability to provide trust, transparency, and strict access control in multi-tenant and dynamic environments. In 5G slicing, where multiple virtual networks coexist on shared infrastructure, ensuring the authenticity and accountability of every transaction and access request is critical. Blockchain technology addresses this by offering a decentralized and immutable ledger to record all slice-related events, such as resource allocations, orchestration activities, and inter-slice communications. This transparency eliminates single points of failure, prevents unauthorized modifications, and allows operators to trace any anomaly to its origin. Moreover, smart contracts automate slice policy enforcement, ensuring that security requirements, service-level agreements, and resource rules are executed without manual intervention, reducing human error and enhancing trust among tenants and service providers.

Together, blockchain and Zero-Trust significantly improve the resilience and integrity of 5G slices. They enable secure multi-party environments where no single entity is fully trusted and all activities are transparently recorded. While challenges such as blockchain's latency and resource overhead persist, integrating lightweight consensus mechanisms and edge-based Zero-Trust enforcement mitigates these issues. As highlighted in the ML-Based 5G Network Slicing Security Survey, combining blockchain, Zero-Trust, and AI-driven monitoring forms a comprehensive defense strategy that protects against attacks, enhances trust, and ensures the secure operation of next-generation 5G networks.

Future Scope

The future of 5G network slicing security lies in the integration of intelligent, adaptive, and automated mechanisms to address evolving threats. Research will increasingly focus on AI- and ML-driven predictive security, enabling real-time anomaly detection and autonomous mitigation. Blockchain and Zero-Trust models will be refined to provide lightweight, scalable solutions for multi-tenant environments, while quantum-resistant encryption will secure communications against future cryptographic attacks. Additionally, as 5G evolves into 6G, attention will shift toward cross-domain slice security, edge computing integration, and IoT protection, ensuring end-to-end resilience. Establishing standardized protocols and global frameworks will be essential for achieving robust and interoperable 5G slice security.

Conclusion

5G network slicing represents a major advancement in mobile communication, enabling highly flexible, efficient, and application-specific virtual networks over shared infrastructure. However, its dynamic and multi-tenant nature introduces complex security challenges, including slice isolation breaches, inter-slice vulnerabilities, resource management risks, and evolving cyber threats. This paper reviewed key concerns and explored comprehensive solutions, including AI-driven anomaly detection, blockchain-based trust management, zero-trust architectures, and secure orchestration frameworks. Machine Learning enhances proactive defense, while blockchain and zero-trust principles provide transparency and continuous verification, collectively strengthening 5G slice security. As networks expand toward 6G, integrating intelligent automation, quantum-resistant encryption, and standardized protocols will become essential for ensuring scalable and interoperable security frameworks. By combining advanced techniques with adaptive policies, 5G network slicing can achieve robust, resilient, and future-ready protection, enabling its full potential across diverse industries while maintaining trust, reliability, and performance.

REFERENCES

[1] Vivek Singh, Manoj Pratap Singh, and Manish Gupta. Security in 5G Network Slices: Concerns and Opportunities. 2024, IEEE Access.

[2] Rutuja Dangi, Akshay Jadhav, Gaurav Choudhary, Nicola Dragoni, Manoj Kumar Mishra, and Punit Lalwani. ML‑Based 5G Network Slicing Security: A Comprehensive Survey. 2022, Future Internet, 14(4), 116. MDPI AG.

[3] Ruxandra Florina Olimid and Gianfranco Nencioni.5G Network Slicing: A Security Overview. 2020, IEEE, University of Bucharest & University of Stavanger.

[4] Josip Lorincz, Amar Kukuruzovi'c and Zoran Blaževi'c, A Comprehensive Overview of Network Slicing for Improving the Energy Efficiency of Fifth-Generation Networks, 2024, Mdpi

[5] Daifallah Alotaibi, Vijey Thayananthan, and Javad Yazdani, The 5G network slicing using SDN based technology for managing network traffic, 2021, Elsevier

[6] Ramraj Dangi, Akshay Jadhav, Gaurav Choudhary, Nicola Dragoni, Manas Kumar Mishra and Praveen Lalwani, ML-Based 5G Network Slicing Security: A Comprehensive Survey, 2022, Mdpi

[7] Wajid Rafique, Joyeeta Rani Barai, Abraham O. Fapojuwo, Life Senior Member, and Diwakar Krishnamurthy, A Survey on Beyond 5G Network Slicing for Smart Cities Applications IEEE,2025

[8] Prashant Subedi, Abeer Alsadoon, P. W. C. Prasad, Sabih Rehman, Nabil Giweli, Muhammad Imran4 and Samrah Arif, Network slicing: a next generation 5G perspective, 2021

[9] Randeep Singh,1 Abolfazl Mehbodniya, Julian L. Webber, Pankaj Dadheech, G. Pavithra, Mohammed S.

Alzaidi, and Reynah Akwafo, Analysis of Network Slicing for Management of 5G Networks Using Machine Learning Techniques 022 Wiley