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

Network Security in 5G - threats, vulnerabilities and mitigation strategies

Hilton Hatitye Chisora [1, *], Munashe Naphtali Mupa [2], Irene Chiedza Chitate [3], Kelvin Gyimah Agyei [4], Ken Mudzingwa [5] and Rodney Chiwanga [6]

[1] *Yeshiva University,*
[2] *Hult International Business School,*
[3] *Arizona State University,*
[4] *University of Memphis,*
[5] *Yeshiva University,*
[6] *Yeshiva University,*

World Journal of Advanced Research and Reviews, 2026, 29(03), 884-895

Publication history: Received on 02 February 2026; revised on 09 March 2026; accepted on 12 March 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0598

Abstract

The implementation of fifth-generation (5G) mobile communication technology can be considered the biggest step in the contemporary global telecommunications environment, as it has better performance potential, a much lower latency rate, and is compatible with a wide range of network devices. Still, this new technology has numerous security risks that should be taken into consideration to ensure the integrity and privacy of the network technologies. The design of 5G network technology shall be used in our research paper to fully indicate the vulnerabilities that arise in the network due to the reliance of the network on software-defined networks, network function virtualisation, and network slicing technology. In addition, the paper also addresses the security issues of the massive attack surface that 5G networks can create, such as the issues of the greater number of devices, edge computing, and supply chains. In order to overcome these security issues in the 5G technology, the paper suggests mechanisms to overcome security vulnerabilities in architectures as well as security at the network level (Singh et al, 2024). A great focus has been put on the security of various components of the 5G network, including core and edge devices and the necessity to take advantage of AI in controlling security threats. Lastly, the paper brings out the relevance of gaps in literature in the field of 5G security, and it is important to note that more studies are needed to come up with effective and scalable security models as 5G technology continues to be implemented in the world today.

Keywords: Mitigation; Network; Security; Threats; Vulnerabilities; 5G

1. Introduction

The emergence of the fifth-generation, or 5G, networks will become the beginning of a telecommunication revolution, which will witness the development of a new paradigm in which the exponentially growing demands of future technologies, including the Internet of Things (IoT), autonomous technology, and smart cities, will be met. The 5G communication technology will be able to support a massive number of gadgets, low latencies, and high-speed data transfer the first time in history. It provides numerous enhanced services, including network slicing, edge computing, and virtualised network functions, which will contribute to the radical change in various significant fields, including the medical, manufacturing, transportation, and entertainment ones.

Nevertheless, with the emergence of such a distributed and complex network paradigm, a multiplicity of cybersecurity issues were generated as well. It is the software-defined nature of 5G networks that are founded on software-defined networking (SDN) and network function virtualisation (NFV) that has enabled the existence of the entirely new

* Corresponding author: Hilton Hatitye Chisora

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

vulnerabilities (Sahu and Pawar, 2022). The network infrastructure is highly vulnerable to cyberattacks affecting the software, APIs, or NFVs, as the network infrastructure is increasingly relying on software. Also, network slicing (when two or more slices of one network are isolated though virtually) to deliver optimum performance based on different requirements is entirely novel threats. Furthermore, the increased quantity of the devices entering the market, especially, the umbrella of the so-called Internet of Things, disproportionately affects the amount of vulnerabilities. Such problems are also complicated by edge computing.

The increasing sophistication of cyber attacks and the increasing dependence of the critical infrastructures increases the necessity to have strong security systems installed in the 5G communication networks. Throughout this paper, we will also endeavour to critically evaluate the main weaknesses and security risks of the 5G network architectures, providing a specific focus on the challenges posed by the convergence of SDN, NFV, network slicing, and edge computing (Sousa & Reis, 2024). The paper shall give a detailed discussion on mitigation measures, which covers a purely technical solution, i.e. application of encryption and access controls, organisational and policy based solutions. Along with the security challenges provided in the paper, there will be practical awareness achievable by the network service providers, security experts, and policymakers to make 5G networks secure.

2. Overview of 5G Architecture and Key Security Features

The fifth generation (5G) networks present the most radical change relative to the previous generations in respect of network structure, speed, and functionality. The fundamental architectural principles of 5G networks are focused on more bandwidth of the network, less network latencies, and the ability to support an exponentially larger number of devices than any other previous generation of network technology (Gantumur, 2024). The greatest architectural innovations of this revolution in network technology include Software-Defined Networking (SDN), Network Functions Virtualisation (NFV), network slicing, edge computing, and service-based architectural innovations. All these innovations have many benefits with regard to high malleability, scalability and efficiency, but they also have new security issues, which are entirely new.

2.1. Core 5G Components

The network 5G architectural model comprises three key elements which are design components of the network, namely the Radio Access Network (RAN), Core Networks and Transport Networks.

- Radio access Network (RAN) - The RAN plays a role in communication between RAN devices such as mobile phones and other IoT devices and the 5G network. Unlike the radio base stations of the past generations, which needed specialised equipment, the RAN in the 5G network will provide scalability and flexibility as the macro cells as well as small cells created using new technologies (Adeosun et al, 2024). Although it provides efficiency in using the spectrum, it has threats associated with interference, rogue base stations, and spoofing attacks.
- Core Network: The 5G core network is the inevitable center, and it deals with traffic, routing data, and supports smooth communication between devices (Bellamkonda, 2021). It is far more cloud-native than its antecedents and based on a service-oriented architecture (SBA), where network functions can be virtualised, and are decoupled with the physical substrate. Virtualising such network functions has the advantage of scaling dynamically and allocating resources; non-the less, issues of security occur because of improper configuration, software vulnerability and absence of adequate isolation between the virtualised network elements.
- Transport Network: This is what will connect the RAN and the core network and will enable the effective transportation of data over 5G network. The network is also low latency and reliable in large data volumes. This network has played a more important role in the use of URLLC, such as autonomous vehicles and remote surgery (Khan et al, 2022). However, the increased complexity of the transport network through cloud infrastructure might cause the development of problems of data integrity and availability, network overload problems in the result of an attack.

2.2. Key 5G Features

One of the most significant aspects of the 5G network is the adoption of the Software-Defined Networking (SDN) paradigm, in which the network can be centrally controlled through software rather than hardware components. In fact, such efficiency can lead to attacks targeting the network control plane, such as Denial-of-Service (DoS) attacks, which can compromise the network controller, or attacks exploiting vulnerabilities in the software-defined network communication interface.

- Network Functions Virtualisation (NFV): NFV can be used to virtualise a network function that could not be virtualised previously. It is possible to implement and manage functions like firewalls, load balancers and routers using commodity hardware and software. Despite the fact that NFV provides the scalability and flexibility necessary to facilitate 5G services, it has some problems in respect of the security, especially in regard to decoupled network functions and hardware. This exposes it to attacks that are directed to the layer of virtualisation or hypervisor.
- Network Slicing: Network slicing is one of the most recent features of the 5G technology, as it facilitates the concept of various network slices or logical partitions that can be executed on the same physical network, which can be adapted to different applications. An example is network slicing, which allows the formation of slices with improved mobile internet and other mission-critical services that require low latency (Triesch et al, 2025). Network slicing has numerous advantages to the technology, but also it creates security concerns associated with network slicing. In fact, the demarcations between network slices must be in such a way so as to provide adequate safeguarding against so-called cross-slice attacks against which a vulnerability in one network slice may have a potential negative impact in other network slices.
- Edge Computing / Multi-Access Edge Computing (MEC): Edge computing allows processing information to be conducted closer to the network edge, and this minimizes latencies and meets real-time application requirements. Especially in the 5G network, the data should be immediately available, which is why edge computing became especially important, such as in the sphere of the augmented reality, autonomous vehicles, or industrial equipment (Ajayi et al, 2024). However, edge computing has several threats, which are more precisely, edge node security, edge data integrity, and edge confidentiality.
- Service-Based Architecture (SBA): The 5G core network applies service-based architectural attributes, with APIs being exploited to raise the number of interactions amongst network functions by additional degrees of modularity and flexibility. This enhances the capability of the network operator to add new services or change the already existing services (Zapata, J.G.). Nevertheless, the presence of these weaknesses in the usage of APIs and WS augments security risks to the integrity of the network depending on security risks associated with appropriate or insufficient use of API services. Such services involve dealing with the security threats associated with the exposure of data or unauthorised access.

2.3. Key Security Features of 5G

The advanced features might be a security issue, but the 5G technology has been enhanced with many features that guarantee improved security over the previous generations. These security advancements in 5G technology comprise:

- Enhanced Authentication and Encryption: The 5G network has a strong authentication of both devices and the network, which involves encryption algorithms, including AES 256-bit encryption (Singh et al, 2024). Moreover, the 5G network guarantees privacy of the subscriber by concealing his or her permanent identifier, SUPI, by temporary identities, SUCI.
- Enhanced Isolation through Network Slicing: Network slicing allows services with different security needs to be deployed and be utilized on the same network without any problems. Network slicing also makes it straightforward to offer isolation between competing or high-priority services, e.g., healthcare or autonomous driving.
- Improved Privacy: 5G technology also represents a number of advantages in regard to consumer privacy safeguarding against surveillance and information disclosure. The network architecture integrates superior privacy features that ensure that the private information of consumers is not intercepted by an unauthorised party.
- Fully Networked Security: 5G: This is one of the advantages of the 5G technology: 5G is able to provide security services as part of the 5G core network (Zapata). This way, the network will be able to offer automated network monitoring services in addition to real-time network threat detection (Kh-Madhloom et al).

These are important improvements, but there is a need to foresee the 5G network in all its perspectives in order to ensure that it is secured. It is connected with the awareness of such problems as network virtualisation, multi-tenancy, inter- devices relations, and so forth. Actually, a strong 5G security must be based on a multi-tier security plan.

3. Security Threats and Vulnerabilities in 5G

The introduction of 5G technology is a new era in mobile communication technology, as it is expected to be faster, have lesser latency, and serve many devices. Nevertheless, these new technologies also have their vulnerabilities that can be exploited. With the 5G network technology, which is also referred to as Software-Defined Networking (SDN), Network Functions Virtualisation (NFV), network slicing, and Edge Computing, the technology is likely to be vulnerable. In this

part, the critical security risks and vulnerabilities related to the 5G technology will be analyzed, both of emerging 5G technologies, and of previous technologies (Ahmad et al, 2024).

3.1. Expanded Attack Surface Due to 5G's Architecture

Besides that, the 5G architectural design introduces new vectors to cyberattacks, most of which are mainly attributed to the spread of these technologies in the new network further. Although these technologies are providing many advantages in terms of flexibility and scalability, it has a number of other vulnerabilities that come along with the following attacks:

- Massive Device Density: The high number of devices projected to register themselves to the 5G network in the form of Internet of Things devices, industrial sensors, autonomous vehicles and mobile devices enhances the surface of attack. Most of these devices, particularly the Internet of Things devices, might not have a powerful processing unit and hence are prone to attack because they might have a poor authentication protocol, weak encryption, or a lack of updated software. An Internet of Things device that has been compromised can be used as a stepping stone to other bigger attacks, including Distributed Denial of Service (DDoS) attacks, or be used to access the main network.
- Virtualisation and Network Functions Virtualisation (NFV): NFV is one of the most important aspects of technological aspects of 5G communication networks. NFV enables the virtualisation of network functions i.e. firewalls or routers that would otherwise be managed via dedicated hardware blocks. Although it enhances the benefits of network management through efficiency and scalability, several security concerns also arise. For example, vulnerabilities may exist in hypervisors or VMS that could allow attackers or cybercriminals to obtain unauthorised access. In addition to that, there are increased threats of "supply chain attacks" through which "malicious code" can get delivered at the "virtualisation layer" and affect the "entire network."
- Software-Defined Networking (SDN): SDN introduces centralised network control through the use of a centralised controller that communicates with network devices, such as routers and switches, using open protocols. Although increased network manageability through SDN enhances network malleability, it also centralises network control, leading to single points of failure. Suppose an attack compromises the network's controller. In that case, it may result in network disruption, manipulation of network routing, or interception of critical data through the potential exploitation of network vulnerabilities. The centralised nature of SDN makes it prone to denial-of-service attacks.

3.2. Vulnerabilities in Network Slicing

Network slicing is one of the most important features of the 5G technology that allows creating several virtual networks, or slices, on the basis of the same physical network. These networks can then be designed to suit the needs of the various use cases including ultra-reliable low-latency communication (URLLC) networks or enhanced mobile broadband (eMBB) networks. Despite the numerous advantages of network slicing as a part of the 5G technology, certain threats are also related to this issue:

- Bad Isolation between Slices: The greatest challenges to the network slicing technology are adequate isolation of network slices. This is to say that the lack of proper isolation controls could allow the party making an attack in one slice of the network to intrude into other slices that have disastrous consequences when there are sensitive information or parts of the mission being considered (Adeosun et al, 2024). As an illustration, in the case of the slice related to the healthcare services industry, the perpetrator party can steal the information of the patients or the medical devices.
- Slice Orchestration and Management Risks: It is not a trivial job to manage the slice itself; and it is mainly dependent on the use of computer-based applications (Alnaim, 2024). An attacker can easily use the vulnerabilities in slice orchestration management system to control the slice in the wrong way and hence cripple the security in cases where vulnerabilities in the slice orchestration management system is present such as in the slice orchestration platforms. Poor security in access or management of the slice may lead to unauthorised access of vital resources.
- Resource Exhaustion and DoS Attacks: Attackers would target individual network slices to send too much traffic or resource request data to them. In turn, this would lead to performance degradation or loss of services. For example, when DDoS attacks target individual network slices, congestion can occur within those slices. In turn, communication services in autonomous vehicles and surgery services in robotics can be affected (De Alwis e al, 2023).

3.3. Edge Computing and MEC Vulnerabilities

Multi-Access Edge Computing (MEC) or edge computing allows the data to be brought nearer to the end user and thus lower latency. However, due to the possibility of edge computing being located across places, there are security concerns of edge computing, such as:

- Physical and Logical Edge services vulnerabilities: MECs are typically implemented in less secure environments than data centres. The edge nodes may be placed in places which are not accessible or audited at all, and they become vulnerable to attacks or unauthorized changes. Moreover, the edge nodes may have the potential of connection to the rest of the network thus the devices may provide an attractive target to the attackers that would want to take advantage of the vulnerabilities in these edge nodes to unauthorised access to data or other network components.
- Data Privacy and Integrity Concerns: Edge computing processes occur near the edge devices and, therefore, require minimal data transfer to both the centralised servers, thus reducing the necessity of transferring data. Though there is the possibility of improving data protection in this manner, there are still some threats of data leakage or alteration during the compromising of edge devices. Hackers may access or modify sensitive data unauthorised or have access to personal or financial information or company secrets.
- Absence of Adequate Security in IoT and Edge Devices: A large number of IoT devices are attached to edge nodes, which do not have proper security. As an example, such tools might not have adequate encryption, have hard-coded passwords, and their software will be obsolete. These security vulnerabilities can be used by an attacker to cause an edge network attack. It is capable of impacting the entire network since the attacker is able to access the MEC server via an unsecured IoT device. Then they will be able to influence the real-time information.

3.4. Supply Chain and Vendor Risks

The 5G technology relies on third-party suppliers, both as hardware, software, and services. The element poses many security threats: though the same could be said about other technologies within the industry.

- Supply Chain Attacks: There are many complex elements of the 5G supply chain, which include network equipment manufacturers down to software and cloud services providers. Any single point of the chain can be compromised by an enemy to either inject vulnerable hardware or software into the supply chain. An example can be when a competitor aims at the hardware supplier to install a hardware backdoor in the hardware, thus gaining the unauthorised access to data or network control.
- Problems with Vendor Trust: It is noteworthy that there are numerous dependencies among various vendors, which creates the issue of security concerns. Each is going to undergo a dissimilar security process and varying degrees of security openness may exist, hence, it may be complicated to guarantee that all of them are implementing stringent security standards. When it comes to network slicing, various vendors might provide various parts of the slice each of which is security mechanism and interface specific.

3.5. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

The network is prone to large scale Denial of Service attacks due to the scalability and inter-connectivity that is brought through the 5G technology, including:

- 5G Networks: Attacks on Control Plane The design of the architecture of 5G networks is complicated. They are susceptible to DDoS attacks because of the centralised character of the control plane, which is being utilised through SDN Controllers and VNFs. Excessing them may cause service outages in large-scale networks particularly in important services like healthcare, transport and utility services. When the control plane is overwhelmed with traffic it may cause disruption in these essential services.
- Adding the New Bells and Whistles of the Networks: The introduction of the new network slicing and edge computing may pose new challenges as the DoS attacks or DDoS attacks. To illustrate this point, the attackers can take advantage of some of the network slices or edge nodes capable of supporting large network traffic resulting in the overloading of resources. Such attacks can be catastrophic in the field of critical applications where the low-latency communication is vital.

3.6. Privacy and Subscriber Identity Issues

5G networks support large amounts of sensitive data, and user privacy protection needs to have a high priority because:

- SUPI/SUCI Exposure: The 5G network will be based on the Subscriber Permanent Identifier (SUPI) that is used to identify its users in a unique manner. Though the use of SUPI can be avoided in 5G security features by means of SUCI whereby encryption is done, there can be instances when the information related to SUPI can be unraveled even under wrong configuration or implementation, thus compromise the privacy of users. Under these circumstances, tracking of users in different networks may occur due to the exposure of SUPI.
- Localisation and Data Breakages: 5G network, together with IoT technology and MEC, allows collecting proper location information, which can be broken by cybercriminals. They are thus able to monitor the activities of individuals or divulge information in regards to important operations, including business operations or government functions.

4. Mitigation Strategies and Best Practices

To address the identified security threats and challenges above, a number of mitigation strategies and best practices will have to be taken. These are as follows, and they must involve variations in architectures down to network-wide controls.

4.1. Architectural and Design-Level Mitigations

- Network Slice Isolation and Security: One of the most critical security aspects at the network level regards proper isolation between network slices. Every slice needs to be considered as if it were an autonomous network. Every slice must have robust security when it comes to accessing the slice. Layers in virtualised environments need to ensure proper isolation between every slice to prevent unauthorised network slice communication. Additionally, every network slice requires robust security during creation and management when utilising the Orchestration tool.
- Embrace Standalone (SA) 5G Networks: Upgrading to standalone 5G network architectures, where the entire 5G network ecosystem operates independently of earlier 4G networks, can help counter security vulnerabilities posed by backward compatibility requirements in current 4G networks. Standalone 5G networks are much more secure than current 4G networks in many aspects. They offer enhanced security capabilities, including end-to-end encryption and advanced identity verification mechanisms.
- Secure SDN and NFV Implementations: With the level of centralisation in the control plane in SDN and the use of network function virtualisation in NFV, there comes the need to ensure secure implementations in these two technologies. For secure implementations of the SDN controller, multi-factor authentication, secure access control mechanisms, and monitoring within the controller are necessary to detect any unusual behaviour. In NFV, there needs to be secure hypervisor implementations to secure against hypervisor escapes and any unauthorised access.
- Edge Computing Security: Edge devices must be secured through robust authentication mechanisms, secure firmware updates, and adequate access controls. Additionally, edge nodes must be segmented from other network components through micro-segmentation methods to prevent edge security vulnerabilities from spreading across the entire network in cases where edge devices are compromised.

4.2. Network-Level Security Controls

- Signalling Firewalls and Intrusion Detection Systems (IDS): The necessity to install signalling firewalls to block malevolent or improperly structured signalling messages in 5G networks cannot be overemphasized because of their communication-intensive nature. IDS and IPS could assist in identifying aberrant behaviour and potential attack in real time. They must be attuned to check and avert network resource assaults in the shape of DoS/DDoS attacks.
- Threat Detection based on AI: AI and ML can help a great deal in real-time threat detection, especially in view of large and dynamic 5G networks. The ML algorithms are able to study the usual patterns of activities within the network and identify anomalies that could be an attempt to attack, e.g., DDoS, exfiltration of data, or unauthorised access. They also can contribute to automation of reaction in real time.
- Zero-Trust Architecture: In order to remove or, at the very least, minimise the unauthorised access, it can be very helpful to apply the zero-trust security paradigm to the 5G network. The application of the zero-trust paradigm where continuous authentication, role-based access, or micro-segmentation are employed within the network can be used to ensure that in case a hacker gains access to one of the network segments, they will have a hard time moving laterally or attaining higher privileges.

4.3. Supply Chain and Vendor Security

- Supply Chain Vetting and Monitoring: To overcome the threats of attack by the supply-chain, all suppliers and third parties service providers must be seriously vetted. Such security verifications must also include periodical security audits, verification of integrity of hardware and software provisions and verification of adherence to secure coding and supply chain security. The operator should also be keen on monitoring networks to make sure that he/she is not trying to compromise the network or its software features.
- Hardware Security and Certification: Certifications of secure Hardware components by the international standards organisation should be compulsory to all critical network components. Such certifications would be able to guarantee that network hardware components do not harbor any form of existing vulnerability or back door. Also, the network hardware devices need regular updates or patches to guard against new threats.

4.4. Privacy and Data Protection

- End-to-End Encryption: This is very important in the sense that all sensitive information passing through the network is encrypted in an end to end manner. It encompasses encryption of signalling messages, SUPI, and user data. That is, the data intercepted will not be readable or editable by the hacker regardless of the number of times it may change hands.
- Data Minimisation and Anonymisation: To ensure that this is not exposed, the data needs to be minimised. By data minimisation, it implies that data relevant to the service delivery must be gathered. Moreover, the information of the subscribers may be anonymized or pseudonymized, in such a way that no attacker can easily identify the person or organisation to which the information belongs.

4.5. Policy and Governance

- Regulatory Compliance: The operator should adhere to all the applicable industry regulations, such as data protection under the GDPR, the NIST Cybersecurity Framework and ITU-T guidelines on 5G security. It will secure the implementation of appropriate security controls within the network, as well as protect the integrity and privacy of data.
- Cross-Sector Collaboration and Threat Intelligence Sharing: Since 5G networks are global, the telecom sector, governments, and technology firms need to co-operate in the exchange of intelligence with regard to threats. Through such collaboration the industry players will be able to come up with collective strategies to counter the threats in the industry since attacks on network security can come at any point in the globalised network. This can also be done by taking measures to standardise security in 5G networks.

4.6. Continuous Monitoring and Incident Response

Real-Time Monitoring and Response to Incidents: To ensure that the security incidents are detected and acted upon when they take place, real-time monitoring of the network is important. It involves tracking network traffic, devices, and network users, to identify any indicators of suspicious behaviour. An incident response plan should be ready in case the security incident happens, and the computer systems that are affected should have to be disconnected off the network immediately and so that post breach, the services should get back to regular operations. Security teams can be trained in the real world attacks by undertaking regular security exercises.

5. Discussion: Challenges and Open Research Areas

Despite the radical enhancement of mobile communication features through the 5G technology, there is a lot of challenge to overcome its use in order to gain security and reliability in the network. The scale, complexity, and connectivity of 5G networks never seen before predetermine the fact that the current situation is conducive to security breaches, and innovative tools and systems are required to address these issues. In this part, the difficulties that communication service providers, researchers, and enterprises are experiencing in achieving 5G networks will be outlined, and substantive areas of research are noted.

5.1. Challenges in Securing 5G Networks

5.1.1. Complexity of the 5G Architecture

The complexities of the 5G architecture that includes SDN, NFV, network slicing, edge computing, and multivendor ecosystems provide a wide range of security threats. As an example, the very concept of 5G, being decentralised, with the size of the attack surface being significant because of the virtualised network functions, could become easily difficult

to control, not to mention securing the 5G as a whole. Traditional security practices do not fit well in such ever-changing environments and the fast speed of 5G activities does not give security structures time to undergo security checks.

5.1.2. Legacy Systems and Hybrid Deployments

The convergence of the past systems is one of the issues posed in the securing of 5G technology, especially in the transition period when the 5G technology will be operating alongside the 4G systems. It will be complicated to secure the weaknesses in the old technology, including legacy 4G, with its low level of encryption and authentication, and therefore prone to cyberattacks (Salahdine et al, 2022). There is also the possibility of jeopardizing the implementation of new security technologies that work in pure 5G settings as a result of the convergence between legacy and new technologies.

5.1.3. Lack of Standardised Security Protocols

Despite certain advances in 5G development, however, the lack of harmonised standards of security is still present across the whole 5G ecosystem. The new security standards have to be developed because of such technologies as network slicing, virtualised network functions, and edge computing. As a matter of fact, currently, disparities in security standards and frameworks in various environments and territories of operators are present, even though such standards are required to guarantee the ability of these technologies to operate in a secure environment.

5.1.4. Increased Attack Surface and Device Proliferation

The quantity of devices to be connected to the network is also one of the most acute security issues in 5G technology, especially because of the blistering growth of the Internet of Things (IoT). The more the devices that are attached to the network, the more the surface area of attack. These devices are in most instances resource-constrained, making them targets of attacks like credential-stuffing attacks, device hijacking, and data exfiltration because of no overall security controls, such as advanced encryption and secure booting. Such devices are easily compromised by a person with the intention of having access to the network. Also, another challenge that is also emerging is security in edge nodes whose environment is less safe since the equipment can provide efficient entry points.

5.1.5. Supply Chain and Vendor Management

The 5G network is based on the support of various suppliers of hardware and software as well as cloud services. All these suppliers might have varying security measures and it could be difficult to ensure that they are all in the same security posture throughout the supply chain. Any security threat to the chain of supply, whether due to defective hardware, vulnerability to software attacks, or the incorrectly established systems, would have flown back. The increased use of open-source elements presents more vulnerability to supply chain compromise, in which malicious hackers can add vulnerabilities at their origin.

5.1.6. Operational and Human Factors

It is important to note that the success of 5G security depends not only on technology but also on dealing with the operation and human factors in the deployment and maintenance of the networks. In fact, the majority of telecommunication companies have difficulties in accessing cybersecurity professionals that would be able to adequately protect 5G networks (Mohan et al, 2022). Secondly, 5G is complicated thus making it difficult to detect, react, and alleviate security events in real-time. Mistakes made by humans such as managing passwords and patch systems may create vulnerabilities that can be easily exploited by an attacker.

5.2. Open Research Areas

5.2.1. AI and Machine Learning for Threat Detection

In 5G network which is dynamic and large-scale, real-time detection of threats becomes more of a challenge. In network security scenarios, researchers can also make their contribution to AI and ML to assist in automating the process of identifying abnormal traffic activity, abnormal behaviour in network functions, or vulnerabilities. It is also possible to use AI to analyse the large amounts of information in real-time in order to identify any anomalies and neutralize new threats.

5.2.2. Zero-Trust Architectures in 5G

The concept of "zero-trust" security, where every request for connectivity is considered "untrusted" until it can be verified as such, has emerged as a crucial methodology in network security. However, achieving zero-trust network

security in 5G communication networks is a complex task in itself, as these networks require ongoing identity verification and management to secure their highly distributed nature (Owoko, 2024). There can, therefore, be research related to scalable architectures in "zero-trust" security in these 5G networks. "Device Authentication," "Network Function Isolation," or "Multi-Tenancy in network slicing" are domains that can lead to innovative research in "zero-trust" security.

5.2.3. Secure Network Slicing and Orchestration

Network slicing is one of the features of the 5G technology. It allows service providers to create various virtual networks that have different requirements concerning the performance, security, and resources. However, the question of a high level of inter-slice isolation is also one of the major challenges of network slicing technology. To mitigate the threats that could cross inter-slices and affect other services, it is important to research new security solutions to slice orchestration, inter-slice access control, and detection.

5.2.4. Edge Security and IoT Integration

As edge computing is implemented in 5G communication, edge security, and IoT devices are included in the network, it needs more research. Research on the security of edge nodes in distributed computing environments processing confidential information and investigation into how edge nodes work under less controlled environments that involve the use of IoT devices is needed. The means of ensuring that edge nodes are safely operated, the integrity of data and their manipulation along the edge must be developed.

5.2.5. Supply Chain Security and Trust Management

The security of both hardware and software of the 5G supply chain is a concern that should be kept putting out fires in the future. Research on the topic of dealing with the problem of trust in engaging with third-party suppliers, conduction of supply chain audit, and the proper implementation of verification will be central in the future. The concept of blockchain technology and its application to the supply chain management and tracing network components is a developing field where better visibility of the hardware or software procurement can be ensured.

5.2.6. Privacy-Enhancing Technologies for 5G

When personal information, such as location, personal communications, and financial transactions, are processed in 5G networks, the question of user privacy is of great concern. To resolve the challenges involving the protection of personal data and at the same time guarantee that the network functions correctly, research on privacy-preserving technologies, including homomorphic encryption, differential privacy, or privacy-preserving machine learning, can be beneficial.

The Interdisciplinary Collaboration of Holistic Security.

There is a need to coordinate the efforts of various industries, such as telecommunications, security, government, and regulatory agencies, when it comes to the security of 5G networks. Investigations concerning structures in cooperation among various areas, like integrated danger insight evaluation, joint security structures, or shared worldwide regulatory treaties may provide considerably better joint security against threats to 5G.

6. Conclusion

The introduction of the 5G technology is a revolutionary shift in the mobile network technology and a massive opportunity to improve communication, the Internet of Things, and innovation in other areas. Simultaneously, the complexity, size, and interconnection of the 5G network technology provides immense security risks. Along with the introduction of new technologies like SDN, NFV, network slicing and edge computing, there are new security vulnerabilities that may be exploited with ease by attackers. Moreover, the sheer amount of devices that are linked to the network amplifies the vulnerability that can be easily exploited by the security threats. The secure network management is difficult with respect to all aspects.

These can be resolved by innovation and also by a joint effort on the part of all stakeholders involved in the telecom, security and regulatory environment. The development of safe 5G networks is guaranteed by research in fields such as AI-based threat analysis, integration of zero-trust networks, safe network slicing, and privacy-saving technology. It is a step to the further evolution in these areas. The growing use of 5G technologies on the international scale demands regular security frameworks every day.

Conclusively, 5G security would be determined by the cooperation of all the stakeholders in ensuring that more security is realised through specific technology creation and the culture of cybersecurity is instilled in the industry. In this way, we will be able to maximize the advantage of 5G technology but will keep safe and reliable the resulting technology together with any data that a technology may operate with. Indeed, the future of 5G security is on the creation of technology that will be strong enough to withstand all threats posed in the future so that the 5G network can give secure coverage in the digital world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] 5G Core Security in Edge Networks: A Vulnerability Assessment Approach — Hisham Kholidy et al., (2023). Focus: Vulnerability assessment methodology (VAA) for 5G core + edge networks, attack graphs, and dynamic analysis. https://www.researchgate.net/profile/Hisham-Kholidy/publication/357065101_5G_Core_Security_in_Edge_Networks_A_Vulnerability_Assessment_Approach/links/64192d55315dfb4cce97a48c/5G-Core-Security-in-Edge-Networks-A-Vulnerability-Assessment-Approach.pdf?origin=publication_detail&utm.

[2] Adeosun, O. A., Fakeyede, M. O., Adesola, A. A., Akingbulere, G., & Anifowoshe, D. O. (2024). Security Implications of network slicing in 5G-Enabled IoT environment. World Journal of Advanced Research and Reviews, 24(03), 2359–2373. https://www.researchgate.net/profile/Adeyemi-Adesola/publication/389267942_Security_implication_of_network_slicing_in_5g-Enabled_IoT_environment/links/67bc1ba4207c0c20fa93f318/Security-implication-of-network-slicing-in-5g-Enabled-IoT-environment.pdf?utm.

[3] Adeosun, O. A., Fakeyede, M. O., Adesola, A. A., Akingbulere, G., & Anifowoshe, D. O. (2024). Security Implications of network slicing in 5G-Enabled IoT environment. World Journal of Advanced Research and Reviews, 24(03), 2359–2373. https://www.researchgate.net/profile/Adeyemi-Adesola/publication/389267942_Security_implication_of_network_slicing_in_5g-Enabled_IoT_environment/links/67bc1ba4207c0c20fa93f318/Security-implication-of-network-slicing-in-5g-Enabled-IoT-environment.pdf?.

[4] Ahmad, I. A. I., Osasona, F., Dawodu, S. O., Obi, O. C., Anyanwu, A. C., & Onwusinkwue, S. (2024). Emerging 5G technology: A review of its far-reaching implications for communication and security. World Journal of Advanced Research and Reviews, 21(1), 2474–2486. https://www.researchgate.net/profile/Michelle-Vivian/publication/390204660_5G_Network_Slicing_Architecture_Implementation_and_Performance_Optimization/links/67e43d71f966c17052a582ee/5G-Network-Slicing-Architecture-Implementation-and-Performance-Optimization.pdf?.

[5] Ajayi, O. O., Chukwurah, N., & Adebayo, A. S. Securing 5G Network Infrastructure From Protocol-Based Attacks and Network Slicing Exploits in Advanced Telecommunications. https://www.researchgate.net/profile/Olanrewaju-Ajayi-2/publication/391439377_Securing_5G_Network_Infrastructure_From_Protocol-Based_Attacks_and_Network_Slicing_Exploits_in_Advanced_Telecommunications/links/68179f6060241d5140227bed/Securing-5G-Network-Infrastructure-From-Protocol-Based-Attacks-and-Network-Slicing-Exploits-in-Advanced-Telecommunications.pdf?.

[6] Alnaim, A. K. (2024). Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security. International Journal of Information Security, 1–21. https://link.springer.com/article/10.1007/s10207-024-00900-5.

[7] Bellamkonda, S. (2021). Strengthening cybersecurity in 5G networks: threats, challenges, and strategic solutions. Journal of Computational Analysis and Applications, 29(6), 1159-1173. https://www.researchgate.net/profile/Srikanth-Bellamkonda-2/publication/385701691_Strengthening_Cybersecurity_in_5G_Networks_Threats_Challenges_and_Strategic_Solutions/links/673176265852dd723cb579cf/Strengthening-Cybersecurity-in-5G-Networks-Threats-Challenges-and-Strategic-Solutions.pdf?utm.

[8] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T. R., & Liyanage, M. (2023). A survey on network slicing security: Attacks, challenges, solutions and research directions. IEEE Communications Surveys & Tutorials, 26(1), 534–570. https://www.researchgate.net/profile/Madhusanka-Liyanage/publication/373143673_A_Survey_on_Network_Slicing_Security_Attacks_Challenges_Solutions_and_Research_Directions/links/64dc7a9325837316ee121670/A-Survey-on-Network-Slicing-Security-Attacks-Challenges-Solutions-and-Research-Directions.pdf?origin=publication_detail&utm.

[9] Gantumur, Z. (2024). Secure Network Slicing in 5G. https://www.researchgate.net/profile/Zoljargal-Gantumur/publication/379084565_Secure_Network_Slicing_in_5G/links/65fab4eaf3b56b5b2d15a6e1/Secure-Network-Slicing-in-5G.pdf?utm.

[10] Khan, M. S., Farzaneh, B., Shahriar, N., Saha, N., & Boutaba, R. (2022, October). SliceSecure: Impact and detection of DoS/DDoS attacks on 5G network slices. In 2022, IEEE Future Networks World Forum (FNWF) (pp. 639–642). IEEE. https://www.researchgate.net/profile/Nashid-Shahriar/publication/369099482_SliceSecure_Impact_and_Detection_of_DoSDDoS_Attacks_on_5G_Network_Slices/links/6436e3144e83cd0e2fab2943/SliceSecure-Impact-and-Detection-of-DoS-DDoS-Attacks-on-5G-Network-Slices.pdf?.

[11] Kh-Madhloom, J., & Alawadi, G. A. H. Literature Review and Exploration: 5G Realm with the Fortifications and Vulnerabilities of Next-Generation Network Security. https://www.researchgate.net/profile/Jamal-Kh-Madhloom/publication/374784664_International_Journal_of_Enterprise_Computing_and_Business_Systems_LITERATURE_REVIEW_AND_EXPLORATION_5G_REALM_WITH_THE_FORTIFICATIONS_AND_VULNERABILITIES_OF_NEXT-GENERATION_NETWORK_SECURITY/links/652fc2e65d51a8012b52baad/International-Journal-of-Enterprise-Computing-and-Business-Systems-LITERATURE-REVIEW-AND-EXPLORATION-5G-REALM-WITH-THE-FORTIFICATIONS-AND-VULNERABILITIES-OF-NEXT-GENERATION-NETWORK-SECURITY.pdf?utm.

[12] Mohan, J. P., Sugunaraj, N., & Ranganathan, P. (2022, May). Cybersecurity threats for 5G networks. In 2022, the IEEE International Conference on Electro Information Technology (eIT) (pp. 446–454). IEEE. https://www.researchgate.net/profile/Niroop-Sugunaraj/publication/361855139_Cyber_Security_Threats_for_5G_Networks/links/6508806961f18040c20b62de/Cyber-Security-Threats-for-5G-Networks.pdf?

[13] Owoko, W. (2024). Exploring the technological advancements and security issues of 5G. World Journal of Advanced Research and Reviews, 23, 812-846. https://www.researchgate.net/profile/Winnie-Owoko/publication/382825410_Exploring_the_Technological_Advancements_and_Security_issues_of_5G/links/67ac47b196e7fb48b9bf1ead/Exploring-the-Technological-Advancements-and-Security-issues-of-5G.pdf?utm.

[14] Sahu, G., & Pawar, S. S. (2022). Security challenges in 5G network. In Software Defined Networking for Ad Hoc Networks (pp. 75–94). Cham: Springer International Publishing. https://www.researchgate.net/profile/Gitimayee-Sahu/publication/358497089_Security_Challenges_in_5G_Network/links/6213081a4be28e145ca636e2/Security-Challenges-in-5G-Network.pdf?utm.

[15] Salahdine, F., Liu, Q., & Han, T. (2022). Towards secure and intelligent network slicing for 5 G networks. IEEE Open Journal of the Computer Society, 3, 23-38. https://www.researchgate.net/profile/Fatima-Salahdine/publication/359389554_Towards_Secure_and_Intelligent_Network_Slicing_for_5G_Networks/links/62e18ed29d410c5ff3695e8a/Towards-Secure-and-Intelligent-Network-Slicing-for-5G-Networks.pdf?.

[16] Singh, V. P., Singh, M. P., Hegde, S., & Gupta, M. (2024). Security in 5 G network slices: Concerns and opportunities. IEEE Access, 12, 52727–52743. https://www.researchgate.net/publication/379715494_Security_in_5G_Network_Slices_Concerns_and_Opportunities/fulltext/6616b98cf7d3fc28743fbe14/Security-in-5G-Network-Slices-Concerns-and-Opportunities.pdf?utm

[17] Singh, V. P., Singh, M. P., Hegde, S., & Gupta, M. (2024). Security in 5 G network slices: Concerns and opportunities. IEEE Access, 12, 52727–52743. https://www.researchgate.net/publication/379715494_Security_in_5G_Network_Slices_Concerns_and_Opportunities/fulltext/6616b98cf7d3fc28743fbe14/Security-in-5G-Network-Slices-Concerns-and-Opportunities.pdf?.

[18] Sousa, A., & Reis, M. J. (2024). 5G Security features, vulnerabilities, threats, and data protection in IoT and Mobile Devices: a systematic review. https://www.researchgate.net/profile/Alexandre-Sousa-23/publication/384095081_5G_Security_Features_Vulnerabilities_Threats_and_Data_Protection_in_IoT_and_Mobile_Devices_A_Systematic_Review/links/6718dd64edbc012ea138af9d/5G-Security-Features-Vulnerabilities-Threats-and-Data-Protection-in-IoT-and-Mobile-Devices-A-Systematic-Review.pdf?.

[19] Triesch, A., Barsch, T., Moonsamy, V., & Große-Kampmann, M. (2025, May). 5G Under Siege: A Comprehensive Guide to Threats and Penetration Testing in 5G Campus Networks. In 2025, International Wireless Communications and Mobile Computing (IWCMC) (pp. 1312–1317). IEEE. https://www.researchgate.net/profile/Matteo-Grosse-Kampmann/publication/390300421_5G_Under_Siege_A_Comprehensive_Guide_to_Threats_and_Penetration_Testing_in_5G_Campus_Networks/links/67e7e61b49e91c0feac4e6f5/5G-Under-Siege-A-Comprehensive-Guide-to-Threats-and-Penetration-Testing-in-5G-Campus-Networks.pdf?utm.

[20] Zapata, J. G. Security Challenges and Solutions for 5G Networks. https://www.researchgate.net/profile/Jannette-Zapata/publication/382641881_Security_Challenges_and_Solutions_for_5G_Networks/links/67cfb14cbab3d32d8440a04c/Security-Challenges-and-Solutions-for-5G-Networks.pdf?.

[21] Zapata, J. G. Security Challenges and Solutions for 5G Networks.