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

Exploring the technological advancements and security issues of 5G

Winnie Owoko *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo, Siaya County, Kenya.

World Journal of Advanced Research and Reviews, 2024, 23(02), 812–846

Publication history: Received on 26 June 2024, revised on 07 August 2024, and accepted on 10 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2367

Abstract

The evolution to fifth-generation (5G) mobile networks marks a transformative era in telecommunications, offering remarkable enhancements in data transfer speeds, reduced latency, and the capability to support an extensive number of connected devices. Despite these advancements, the rapid deployment of 5G technology introduces significant security and privacy challenges. This paper seeks to address the problem of securing 5G networks against potential vulnerabilities and cyber-attacks, which could undermine the reliability and integrity of this critical infrastructure. Previous efforts to mitigate these security issues have focused on enhancing encryption methods, developing robust authentication protocols, and implementing advanced intrusion detection systems. However, these approaches often fall short due to the complex and dynamic nature of 5G networks, which incorporate diverse technologies and a wide range of frequency bands. This study identifies the limitations of existing solutions, such as their inability to adequately protect against sophisticated attacks and their lack of scalability in the face of rapidly expanding network demands. To address these challenges, this paper employs a multi-faceted methodology, including a comprehensive review of current security practices, a detailed analysis of potential vulnerabilities within 5G architecture, and the development of innovative security frameworks tailored specifically for 5G networks. The research includes both theoretical models and practical simulations to validate the proposed solutions. The results indicate significant improvements in the security and resilience of 5G networks, with the proposed frameworks effectively mitigating identified vulnerabilities and enhancing overall network protection. These findings have important implications for the future of telecommunications, suggesting that with the right security measures, 5G can be safely and effectively integrated into critical infrastructure, supporting innovations in smart cities, autonomous vehicles, and industrial automation.

Keywords: 5G technology; Security issues; Privacy concerns; Cybersecurity; Data privacy; Telecommunications

1. Introduction

Mobile networks, which have a 40-year history that parallels the Internet's, have undergone significant change. The first two generations supported voice and then text, with 3G defining the transition to broadband access, supporting data rates measured in hundreds of kilobits per second. Today, the industry is transitioning from 4G (with data rates typically measured in the few megabits per second) to 5G, with the promise of a tenfold increase in data rates [1]-[5]. The fifth generation (5G) of mobile networks represents a substantial technological advancement over its predecessors, delivering significant improvements in several key areas that enhance both user experience and the functionality of connected devices [6]-[10]. Enhanced connectivity is one of the hallmarks of 5G, providing broad coverage that ensures connectivity in both urban and rural areas. This extensive coverage is essential for connecting devices in remote locations and supporting applications that require continuous connectivity, such as autonomous vehicles. Additionally, 5G networks offer higher reliability, reducing the likelihood of dropped connections and ensuring more consistent performance, which is critical for applications like telemedicine [11] and the remote control of industrial machinery. 5G offers data transfer rates that are exponentially faster than those of 4G LTE, with users experiencing download speeds of up to 10 Gbps [12]. This increase in speed enables high-definition video streaming, rapid file downloads, and smooth

* Corresponding author: Winnie Owoko

online gaming. The increased bandwidth capacity of 5G networks supports more simultaneous connections and higher data rates, essential for handling the vast amount of data generated by IoT devices [13]-[16]. This expansion in bandwidth [17] facilitates the seamless integration of various connected devices and services, making it a cornerstone for modern digital infrastructure. One of the most significant advancements of 5G technology is its ability to reduce latency to as low as one millisecond, compared to around 50 milliseconds for 4G [18]. This near-instantaneous communication is crucial for applications requiring real-time responsiveness, such as autonomous driving, remote surgery, and virtual reality (VR) experiences [19]-[22]. The reduction in latency enhances user experience by minimizing delays in communication and interaction, making applications like video conferencing more seamless and interactive. This improvement is vital for developing and implementing technologies that rely on quick and reliable data transmission [23].

5G networks are built to handle the explosion of IoT devices, including smart home devices, industrial sensors, and wearable technology [24], [25]. With the ability to support up to one million devices per square kilometer, 5G can manage the connectivity needs of dense urban environments and large-scale industrial operations [26]. Network slicing technology allows the creation of multiple virtual networks within a single physical 5G network, each optimized for specific types of services and applications [27], [28]. For example, one slice can be dedicated to low-latency [29] applications like autonomous vehicles, while another can cater to high-bandwidth applications like streaming services. Figure 1 presents the critical timelines in the evolution of mobile networks.

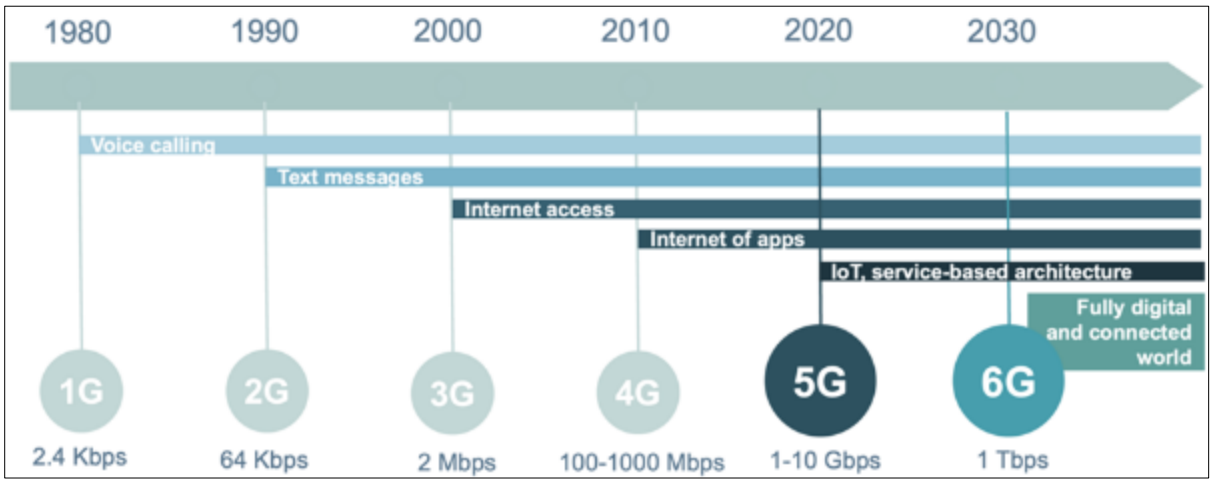


Figure 1 History of Mobile Networks

The facilitation of emerging technologies is another critical aspect of 5G. It is pivotal in enabling the IoT ecosystem by providing the connectivity required for a vast array of devices to communicate and operate effectively. This connectivity supports smart homes, smart cities, and various industrial IoT applications [30]. 5G technology is essential for developing smart cities, where connected infrastructure and services can improve urban living. This includes intelligent traffic management systems, enhanced public safety through surveillance and emergency response systems, and efficient utility management [31]-[35]. The low latency and high reliability of 5G networks are critical for the safe operation of autonomous vehicles, which rely on real-time data exchange for navigation, collision avoidance, and communication with other vehicles and infrastructure. Furthermore, 5G enables advanced industrial automation by providing robust and low-latency connectivity for industrial robots, remote monitoring, and control systems, facilitating smarter manufacturing processes, predictive maintenance, and overall operational efficiency. Figure 2 shows the various use cases of 5G technologies.

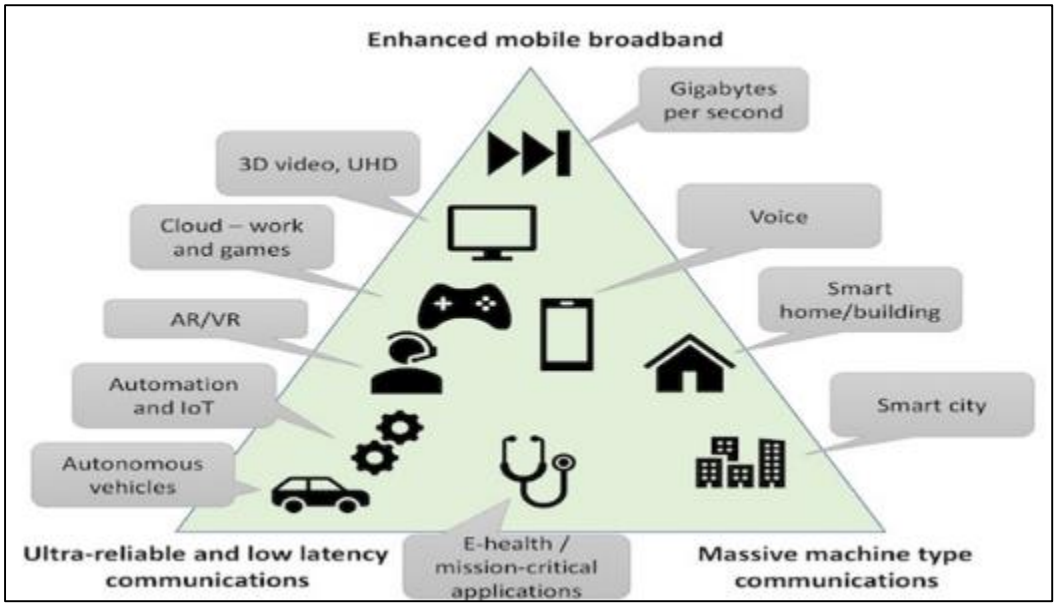


Figure 2 5G use cases

5G networks offer transformative advancements over previous generations by providing enhanced connectivity, higher speeds, lower latency, and the ability to support a massive number of connected devices [36]. These improvements are not only beneficial for mobile broadband but are also crucial for the successful implementation and operation of the Internet of Things (IoT), smart cities, autonomous vehicles, and industrial automation, driving innovation and efficiency across various sectors [37]-[41].

As 5G technology becomes increasingly integrated into various aspects of daily life and critical infrastructure, ensuring user privacy becomes paramount [42], [43]. The enhanced capabilities of 5G networks, including higher speeds, lower latency, and the capacity to support a massive number of connected devices, come with a significant increase in data transmission and collection. This vast data flow includes personal information, location data, and sensitive financial details, which are all highly attractive targets for cyber-attacks and privacy breaches [44]-[47].

The problem under investigation is the heightened vulnerability of user data in 5G networks. Unlike previous generations, 5G networks not only connect mobile devices but also facilitate the Internet of Things (IoT), smart cities, autonomous vehicles, and industrial automation [48],[49]. This expansive connectivity means that any security lapse can have far-reaching consequences, impacting not just individual users but entire communities and critical infrastructure systems. The implications of such breaches include identity theft, financial fraud, unauthorized surveillance, and disruptions to essential services.

Cybercriminals are becoming more sophisticated, exploiting vulnerabilities in these advanced networks to access and misuse personal data [50]-[53]. The sheer volume and variety of data transmitted through 5G networks create numerous entry points for attackers. Moreover, the complexity of 5G architecture, with its diverse range of connected devices and services, makes securing the network a daunting task [54]. Traditional security measures are often insufficient, requiring more robust and innovative approaches to protect user data.

This problem is worthy of solving because the success and widespread adoption of 5G technology hinge on user trust. Without robust privacy protections, users may be reluctant to embrace 5G services [55], hindering technological progress and economic growth. Ensuring data privacy in 5G networks is not just about safeguarding personal information; it's about securing the foundation of future technological advancements that promise to revolutionize industries, improve public services, and enhance quality of life.

To address these challenges, this work makes several major contributions:

- Identification of Primary Privacy Concerns: This research identifies and categorizes the main privacy issues inherent in 5G networks, providing a comprehensive understanding of the risks involved.

- Comparison with Previous Generations: The study highlights how privacy concerns in 5G differ from those in earlier mobile network generations, emphasizing the unique challenges posed by 5G.
- Evaluation of Existing Solutions: The research examines current technologies and protocols designed to address privacy issues in 5G networks, assessing their effectiveness and limitations.
- Recommendations for Best Practices: Based on the findings, the study proposes best practices and strategies to enhance user data protection in 5G networks, aiming to provide actionable guidelines for stakeholders.
- Case Studies of Data Breaches: The research includes case studies of notable data breaches in telecom networks, offering insights into the nature of these incidents and their impacts, and highlighting the importance of robust privacy protections.
- Mitigation Strategies: The study outlines specific mitigation strategies to address identified privacy concerns, focusing on advanced encryption methods, dynamic pseudonymization, multi-factor authentication, and secure cloud configurations.

By tackling these critical issues, this work aims to contribute to the secure and trustworthy adoption of 5G technology, ensuring that its benefits can be fully realized without compromising user privacy.

2. Methodology

2.1. Research Design

This study employs a mixed-methods approach, combining systematic literature review, case studies, and content analysis to investigate the privacy concerns and performance issues in 5G networks. This comprehensive approach allows for a thorough examination of both theoretical and practical aspects, providing a robust framework for identifying vulnerabilities and proposing innovative solutions.

2.2. Data Sources

The primary data sources for this research include peer-reviewed academic journals, industry white papers, technical documents, and reports from authoritative bodies relevant to 5G networks, cybersecurity, and telecommunications infrastructure. Key databases such as IEEE Xplore, ScienceDirect, SpringerLink, Wiley Online Library, and Google Scholar are utilized to ensure the collection of high-quality and relevant literature. Additionally, reports from organizations like the International Telecommunication Union (ITU), the European Union Agency for Cybersecurity (ENISA), and major telecommunication companies are included to capture a wide range of perspectives and insights.

2.3. Search Strategy

A strategic and systematic search is conducted using specific keywords and phrases related to 5G privacy issues, network performance challenges, and mitigation strategies. Keywords such as "5G privacy concerns," ” 5G security concerns,” "5G performance issues," "5G network optimization," "encryption in 5G," and "5G case studies" are used, with Boolean operators (AND, OR) to refine search results. The search is comprehensive, covering titles, abstracts, and keywords, and focuses on literature published from 2010 to 2024 to capture recent developments and trends in the field.

2.4. Inclusion and Exclusion Criteria

Inclusion criteria for this study consist of peer-reviewed articles, conference papers, industry reports, and technical documents published between 2010 and 2024, specifically addressing the privacy and performance aspects of 5G networks. Only English-language publications are considered to maintain consistency in analysis. Exclusion criteria include studies that do not directly address privacy concerns or performance issues in 5G networks, non-English publications, and articles outside the specified timeframe.

2.5. Selection Process

The selection process involves an initial screening of titles and abstracts to identify potentially relevant studies, followed by a thorough full-text review to confirm eligibility based on the defined criteria.

2.6. Data Analysis

Data analysis involves a combination of content analysis and thematic synthesis. Content analysis is conducted on the selected literature and case study data to extract relevant information on privacy vulnerabilities, performance challenges, and mitigation strategies. The analysis focuses on identifying key themes, patterns, and gaps in existing

knowledge. Thematic synthesis is then used to integrate findings from different sources, highlighting critical aspects of 5G privacy and performance issues.

2.7. Synthesis and Recommendations

The findings from the literature review and case studies are synthesized to provide a comprehensive understanding of the current state of privacy and performance challenges in 5G networks. Based on this synthesis, the study proposes innovative strategies and solutions to enhance the security, privacy and performance of 5G networks. Recommendations are tailored to address technical, policy, and capacity-building aspects, ensuring a holistic approach to mitigating privacy concerns and optimizing network performance in 5G infrastructure.

3. 5G network architecture

The 5G core network, which provides coordination between different parts of the access network and connectivity to the internet, is a service-based architecture (SBA) built around cloud-based technologies and provides authentication, security and session management, as well as other functions and services. 5G creates a dynamic, coherent, and flexible framework of advanced technologies to support a variety of applications [56], [57]. 5G utilizes a more intelligent architecture, with Radio Access Networks (RANs) no longer constrained by base station proximity or complex infrastructure. 5G leads the way towards disaggregated, flexible, and virtual RAN with new interfaces creating additional data access points (5). Figure 2 shows a typical 5G network architecture.

3.1. 5G RAN (Radio Access Network)

The Radio Access Network (RAN) is a crucial component of 5G architecture, responsible for connecting user devices to the core network. One of the significant advancements in 5G RAN is the introduction of the 5G New Radio (NR) interface [58]. 5G NR supports a broad range of frequencies, from low-band (sub-1 GHz) to mid-band (1-6 GHz) and high-band (millimeter waves above 24 GHz), enabling higher data rates and more robust connections. The use of millimeter waves, in particular, allows for much larger bandwidths compared to previous generations, facilitating ultra-high-speed data transmission necessary for applications such as virtual reality and high-definition video streaming [59], [60]. The 5G RAN is a crucial component of 5G networks, providing the wireless connection between user devices and the core network. It consists of various elements like base stations, antennas, and radio units that facilitate the high-speed, low-latency communication necessary for 5G. 5G RAN supports advanced technologies such as massive MIMO (Multiple Input Multiple Output), which increases capacity and coverage, and beamforming, which directs signals more precisely. It operates across a wider range of frequency bands, including mmWave, to deliver significantly faster data rates and improved network efficiency compared to previous generations. This network architecture enables diverse applications, from enhanced mobile broadband to IoT and mission-critical services. Figure 3 shows the basic 5G network architecture.

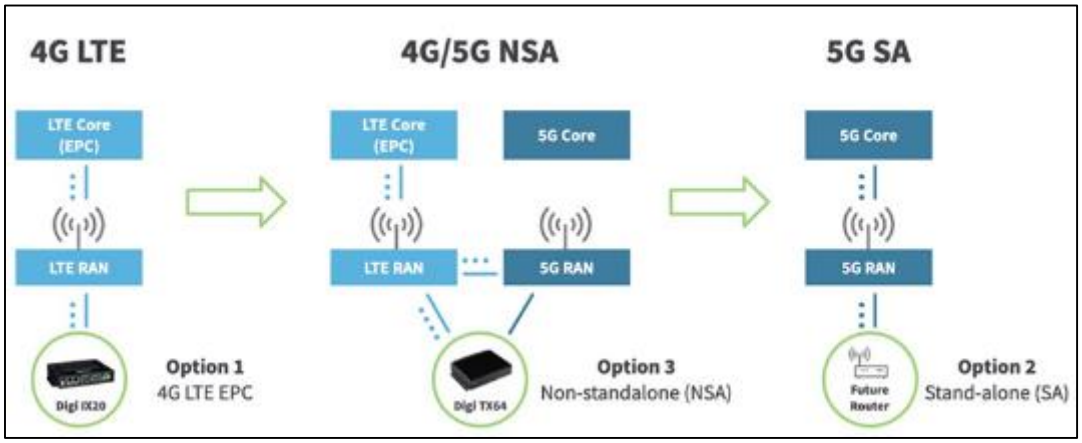
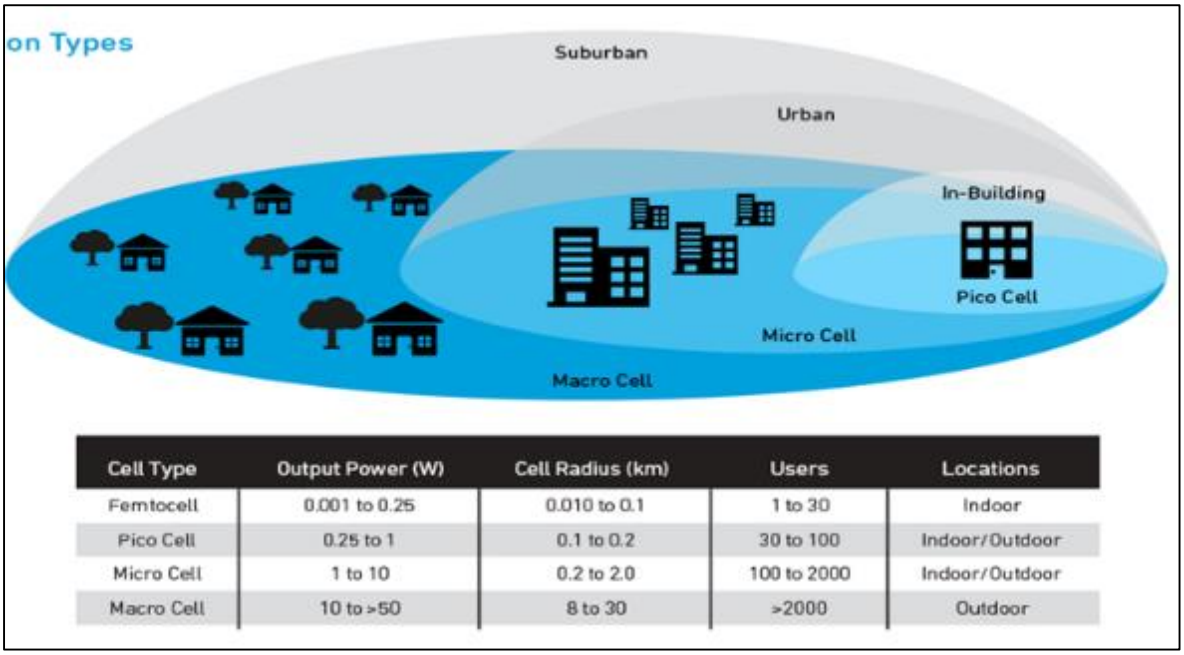


Figure 3 5G network architecture

Small cells play a pivotal role in the 5G RAN by enhancing network coverage and capacity, especially in densely populated urban areas. Unlike traditional macro cells that cover large geographical areas, small cells have a limited range, making them ideal for providing targeted coverage and capacity in high-demand locations like stadiums, shopping malls, and city centers [61], [62]. This dense deployment of small cells helps to offload traffic from macro cells, improving overall network efficiency and user experience. Figure 4 illustrates the different cells in 5G networks.



Cell Type	Output Power (W)	Cell Radius (km)	Users	Locations
Femtocell	0.001 to 0.25	0.010 to 0.1	1 to 30	Indoor
Pico Cell	0.25 to 1	0.1 to 0.2	30 to 100	Indoor/Outdoor
Micro Cell	1 to 10	0.2 to 2.0	100 to 2000	Indoor/Outdoor
Macro Cell	10 to >50	8 to 30	>2000	Outdoor

Figure 4 Types of Small cells

Massive Multiple Input Multiple Output (MIMO) technology is another key feature of 5G RAN [63], [64]. Massive MIMO involves the use of a large number of antennas at the base station to simultaneously serve multiple users, significantly increasing spectral efficiency and throughput. By leveraging advanced antenna techniques, such as spatial multiplexing and beamforming, massive MIMO enhances the capacity and reliability [65] of wireless communication. Beamforming, in particular, focuses the wireless signal in specific directions rather than broadcasting it in all directions, reducing interference and improving signal quality for the end-users.

3.2. 5G Core Network

The 5G core network is the heart of 5G networking, it provides secure and reliable connectivity to the internet and access to all of the networking services [66]. 5G core network has numerous essential functions for mobile networking like mobile management, subscriber data management, authorization, authentication policy management [67]. The 5G core network is completely software-based [68] and native to the cloud, it allows higher deployment agility and has flexibility and infrastructure which is similar to the cloud. Industry experts designed the 5G core to support the network functioning of the 5G network. Therefore, the 3GPP standard was developed which was named 5G core [69], it has the power to control and manage network functions.The core network in 5G architecture represents a departure from the traditional, hardware-centric approach used in previous generations. At the heart of the 5G core is the Service-Based Architecture (SBA), which employs a service-oriented design to enhance flexibility and efficiency [70], [71]. SBA decouples network functions from the underlying hardware, allowing them to run as modular, virtualized services. This modularity facilitates more efficient resource utilization [72] and simplifies network management, enabling operators to deploy and scale services more dynamically. Network Functions Virtualization (NFV) is a key technology underpinning the 5G core network [73] as shown in Figure 5. NFV separates network functions such as routing, firewalling, and load balancing from proprietary hardware and implements them as software applications that can run on standard servers [74]-[77]. This virtualization reduces the dependency on specialized hardware, lowering costs and increasing the agility of network deployments. By leveraging NFV, operators can quickly introduce new services and adapt to changing demands, enhancing the overall scalability [78] and flexibility of the network.

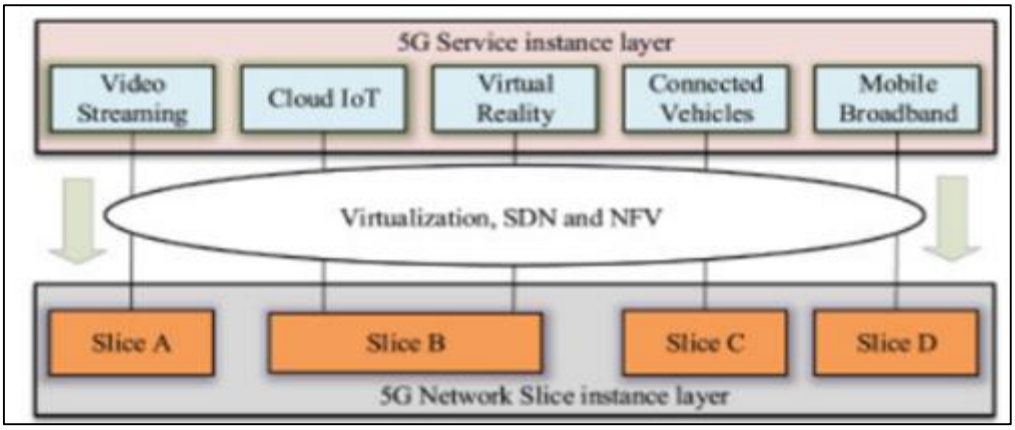


Figure 5 Network functions virtualization

Software-Defined Networking (SDN) complements NFV by providing a centralized, programmable control plane that can dynamically manage and optimize network resources [79], as shown in Figure 6. SDN separates the control plane, which makes decisions about how to route traffic, from the data plane, which actually forwards the traffic [80]-[83]. This separation allows for more granular control over network behavior and facilitates the implementation of policies that can enhance performance, security, and reliability. In a 5G network, SDN can be used to create virtual network slices, each tailored to meet the specific requirements of different applications or services, such as enhanced mobile broadband (eMBB), ultra-reliable low latency [84] communications (URLLC), or massive machine-type communications (mMTC).

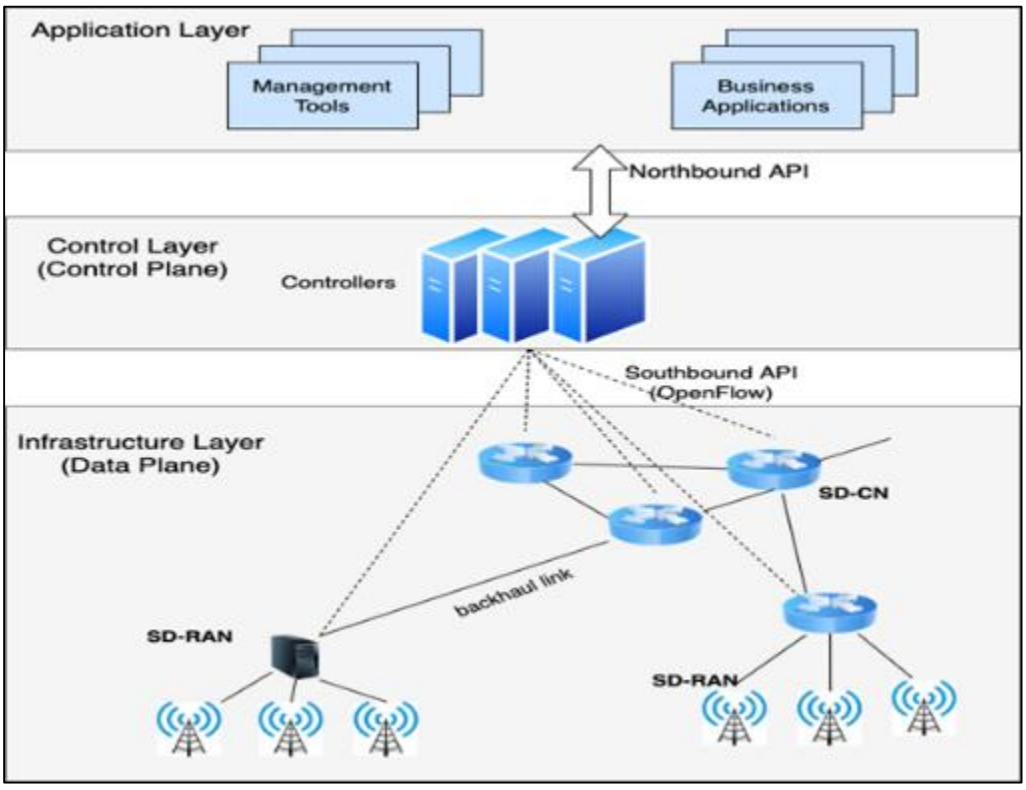


Figure 6 Software-Defined 5G Network Architecture

Network slicing is a revolutionary concept enabled by SDN and NFV in the 5G core network [85] as shown in Figure 7. It involves creating multiple virtual networks within a single physical infrastructure, each optimized for specific use cases. For instance, a network slice can be customized to provide ultra-low latency for autonomous vehicles, while another slice can offer high bandwidth for streaming services [86]-[89]. This level of customization ensures that the diverse requirements of various applications are met efficiently, without compromising on performance or security.

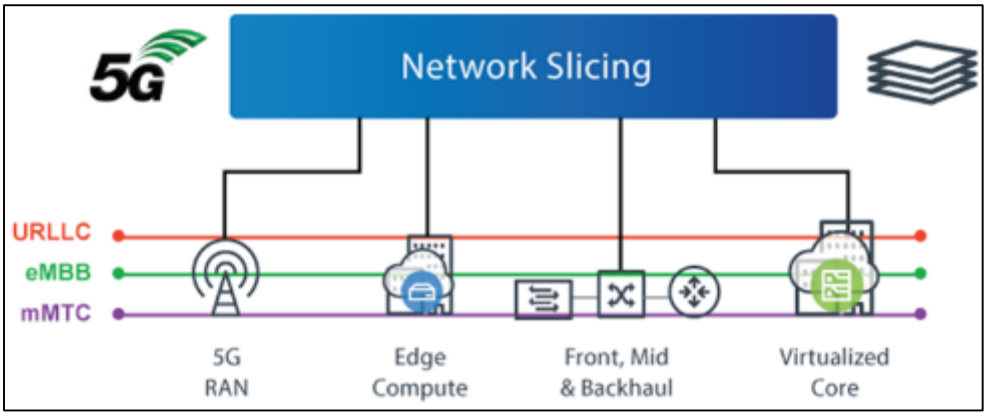


Figure 7 Network slicing

By integrating these advanced technologies, the 5G core network not only enhances the overall efficiency [90] and flexibility of the network but also provides the foundation for innovative services and applications that can drive economic growth and improve quality of life.

4. Security issues in 5G networks

5G security is a crucial aspect of wireless network security that specifically addresses the unique challenges posed by fifth-generation (5G) wireless networks [91]. The advanced capabilities of 5G, including enhanced speed, lower latency, and support for a massive number of connected devices, require robust security technologies to protect both the infrastructure and the 5G-enabled devices [92]-[95]. These technologies are designed to safeguard against data loss, cyberattacks, hackers, malware, and other threats. Unlike previous generations, 5G extensively utilizes virtualization, network slicing, and software-defined networking (SDN), which introduce new vulnerabilities [96] and potential attack vectors. Consequently, securing 5G networks involves addressing these sophisticated and emerging threats to ensure the integrity, confidentiality, and availability of data transmitted across the network. Virtualization decouples network functions from physical hardware, allowing for more flexible and dynamic network management, but also introduces vulnerabilities related to hypervisors and virtual machines [97]. Network slicing enables the creation of multiple virtual networks on a shared physical infrastructure, each tailored for specific applications or services. While this improves efficiency, it also raises concerns about ensuring the isolation and integrity of each slice to prevent cross-contamination and unauthorized access [98]-[100].

5G's reliance on a wide range of frequency bands, including higher frequency millimeter waves, expands the attack surface, making it more susceptible to physical layer attacks like jamming and eavesdropping [101], [102]. The sheer number of connected devices in 5G, especially with the proliferation of IoT devices, increases the potential entry points for cyberattacks, necessitating more robust authentication and encryption mechanisms to secure communications [103], [104]. Moreover, the integration of 5G into critical infrastructure and essential services amplifies the risks associated with potential security breaches, making it imperative to adopt comprehensive and adaptive security measures to address these evolving threats. Supply chain security is another critical concern in 5G networks. The global nature of 5G equipment manufacturing and deployment increases the risk of compromised components being introduced into the network, which can be exploited by malicious actors [105]. Ensuring the security and integrity of these components is essential to prevent backdoors and other forms of hardware tampering.

Moreover, the high-speed and low-latency capabilities of 5G [106] make it an attractive target for advanced persistent threats (APTs) and other sophisticated cyberattacks. Protecting against these threats requires continuous monitoring, advanced threat detection, and rapid response capabilities. Overall, addressing these security issues in 5G networks is vital to ensure the safe and reliable operation of this transformative technology. As explained in [107], 5G networks represent a significant leap forward in telecommunications, promising faster speeds, lower latency, and the capacity to connect a vast number of devices. However, these advancements come with an array of security challenges [108]. Table 1 presents an extensive discussion of the security issues in 5G networks.

Table 1 Security issues in 5G networks

Security issue	Details
Increased Attack Surface	*More Devices*: With the Internet of Things (IoT), 5G will connect billions of devices, increasing the potential entry points for attackers [109], [110].
	Network Slicing: 5G enables network slicing, which allows multiple virtual networks to operate on a single physical infrastructure. While this improves efficiency, it also complicates security, as each slice must be secured independently [111], [112].
	Diverse Use Cases: The use cases for 5G, from autonomous vehicles to smart cities, introduce varied security requirements and challenges [113], [114].
Software-Defined Networking (SDN) and Network Function Virtualization (NFV)	*Centralized Control:* SDN centralizes control functions, which, if compromised, can lead to widespread network disruption [115], [116].
	Virtualization Risks: NFV replaces dedicated hardware with software running on general-purpose hardware, increasing the potential for software vulnerabilities [117], [118].
Advanced Persistent Threats (APTs)	APTs are sophisticated, multi-phase attacks aimed at persistent access to networks [119]. 5G's complexity and increased reliance on software make it a prime target for such attacks.
Supply Chain Security	5G networks rely on a global supply chain, including hardware and software from various vendors [120]. This introduces risks of counterfeit components, malicious software, and compromised manufacturing processes.
Authentication and Identity Management	*Device Authentication:* With billions of connected devices, ensuring secure and efficient device authentication [121] becomes challenging.
	User Privacy: Stronger authentication mechanisms are needed to protect user identities and prevent unauthorized access [122], [123].
Data Privacy	*Data Collection:* 5G will enable extensive data collection from numerous devices, raising concerns about user privacy and data protection [124]-[127].
	Data Transmission: Protecting data in transit across diverse and dynamic 5G networks is crucial to prevent eavesdropping and data breaches [128].
Denial of Service (DoS) Attacks	5G networks, with their critical applications, are prime targets for DoS attacks, which can cripple services like autonomous driving and smart infrastructure [129], [130].
Interoperability and Legacy Systems	Integrating 5G with existing 4G and older networks introduces compatibility and security issues [131]. Legacy systems may have vulnerabilities that can be exploited when interconnected with 5G.
Physical Security	5G infrastructure, including base stations and data centers, must be protected against physical attacks, such as tampering or sabotage [132], [133].
Regulatory and Compliance Challenges	*Global Standards:* The global nature of 5G requires consistent security standards and regulations [134], which can be difficult to implement across different jurisdictions.
	Compliance: Ensuring compliance with data protection laws (e.g., GDPR) and other regulatory requirements adds complexity to 5G security [135].
Artificial Intelligence (AI) and Machine Learning (ML) Threats	While AI and ML can enhance security through advanced threat detection, they can also be used by attackers to develop more sophisticated attacks [136].
Zero Trust Architecture	Implementing a zero-trust security model [137] in 5G networks, where no device or user is trusted by default, is essential but challenging due to the network's complexity and scale.

The transition to 5G networks presents significant security challenges that require a multi-faceted and proactive approach [138], [139]. By addressing these issues comprehensively, stakeholders can harness the full potential of 5G while safeguarding against potential threats.

5. Privacy issues in 5G networks

The integration of 5G into various facets of daily life and critical infrastructure also raises significant privacy concerns. One of the primary issues is the sheer volume and granularity of data collected and transmitted by 5G networks [140], [141]. With enhanced capabilities for real-time data processing and high-speed communication, 5G networks handle a vast amount of personal and sensitive information, making them attractive targets for cyber-attacks and privacy breaches [142]-[145]. Protecting this data is essential not only for safeguarding individual privacy but also for maintaining user trust and ensuring the secure adoption of 5G technology. These concerns span across data confidentiality, user identity protection, and secure data transmission. Table 2 below explores these issues in detail, examining their implications and potential solutions.

Table 2 Analysis of privacy concerns

Privacy Concern	Issue	Implications
Data Confidentiality	Increased opportunities for data breaches and unauthorized access due to higher data throughput in 5G.	Exposure of sensitive personal and financial information, increased risk of data interception.
User Identity Protection	Susceptibility of user identity and location information to tracking and profiling.	Privacy invasions, stalking, misuse of personal information, increased risk of targeted attacks and surveillance.
Secure Data Transmission	Complexity in ensuring secure data transmission across various nodes and devices in 5G networks.	Data interception, tampering, and man-in-the-middle attacks, compromising data integrity and confidentiality.
Privacy-Preserving Data Analytics	Challenges in performing data analytics on 5G-generated data while preserving user privacy.	Exposure of sensitive information during analytics, leading to privacy violations and reduced user trust in 5G services.

Addressing privacy issues in 5G networks is also crucial for regulatory compliance. Various privacy laws and regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), impose stringent requirements on how personal data is collected, processed, and stored. Ensuring that 5G networks comply with these regulations is vital to avoid legal repercussions and foster a trustworthy digital ecosystem.

Recent years have seen several high-profile data breaches in telecom networks, underscoring the critical need for robust privacy protections. Table 3 examines notable case studies of privacy breaches, highlighting the nature of these incidents, and their impacts. These case studies provide valuable insights into the vulnerabilities within telecom networks and the essential strategies needed to mitigate these risks, ensuring a secure and trustworthy 5G environment.

Table 3 Privacy Concerns Case Studies

Case Study	Description	Impact
T-Mobile Data Breach (2021)	In August 2021, T-Mobile experienced a major data breach where hackers accessed personal data of over 40 million former and prospective customers and 7.8 million current postpaid customers. Data included names, dates of birth, Social Security numbers, driver's license/ID information, and more.	Significant loss of customer trust, potential financial fraud, regulatory scrutiny, and substantial fines.
Vodafone Italy Data Breach (2022)	In May 2022, Vodafone Italy reported a data breach affecting 2.5 million customers, where attackers accessed names, phone numbers, and addresses.	Compromise of personal data, leading to privacy violations and potential phishing attacks.

Verizon Data Exposure (2023)	In June 2023, a misconfigured cloud storage bucket exposed sensitive customer data, including names, addresses, account details, and account PINs for millions of Verizon customers.	Exposure of sensitive data, leading to potential identity theft and financial fraud.
BT (British Telecom) Cyber Attack (2024)	In March 2024, BT suffered a cyber-attack where hackers accessed the personal data of approximately 5 million customers, including names, addresses, phone numbers, and email addresses.	Data breach leading to privacy invasion, regulatory investigations, and potential financial losses.

5G networks, with their advanced capabilities and extensive connectivity, present numerous privacy issues that need careful consideration. Table 4 presents an extensive discussion of the privacy challenges in 5G networks:

Table 4 Privacy challenges in 5G networks

Privacy issue	**Details**
Increased Data Collection	*Volume and Variety:* 5G networks will enable a vast array of connected devices, from smartphones to smart home devices, each collecting large amounts of data [146], [147]. This data can include sensitive personal information, location data, and usage patterns.
	Detailed User Profiles: The sheer volume of data collected can be used to create detailed user profiles, potentially leading to privacy invasion if this information is misused or falls into the wrong hands [148].
Location Tracking	*Precision:* 5G networks offer high-precision location tracking, which can be beneficial for services like navigation but poses significant privacy risks [149]-[151]. Detailed location data can reveal a lot about an individual's habits, preferences, and routines.
	Continuous Monitoring: Continuous location tracking can lead to constant surveillance [152], raising concerns about individuals' privacy and autonomy.
Interconnected Devices and IoT	*Device Ecosystem:* The Internet of Things (IoT) will see an explosion of connected devices, from wearables to smart appliances, all communicating over 5G [153]. Each device can collect and share personal data, increasing the potential for privacy breaches [154].
	Data Aggregation: Aggregating data from multiple devices can provide a comprehensive picture of an individual's life, raising concerns about how this data is used and who has access to it [155], [156].
Data Transmission and Storage	*In-Transit Data:* Data transmitted over 5G networks, if not properly encrypted, can be intercepted [157] and accessed by unauthorized parties.
	Cloud Storage: Much of the data generated by 5G devices will be stored in the cloud, introducing risks related to cloud security and data breaches [158].
User Consent and Control	*Informed Consent:* Ensuring users are fully informed about what data is being collected [159], how it is used, and who it is shared with is challenging in the complex 5G ecosystem.
	Data Control: Users often have limited control over their data once it is collected [160]. They may not be able to delete or manage this data effectively, leading to potential misuse.
Network Slicing	*Isolated Environments:* Network slicing allows the creation of isolated virtual networks for specific use cases. While beneficial, it complicates privacy management as each slice may have different privacy requirements and controls [161].
	Data Segregation: Ensuring proper data segregation and privacy within each network slice is crucial to prevent data leakage between slices [162].
Cross-Border Data Transfers	*Global Networks:* 5G networks are inherently global, leading to data being transferred across borders. This raises issues related to differing privacy [163] regulations and protections in various jurisdictions.
	Compliance: Ensuring compliance with privacy laws like the General Data Protection Regulation (GDPR) when data is transferred internationally is a complex challenge [164].

Artificial Intelligence (AI) and Machine Learning (ML)	*Data Usage:* AI and ML technologies used in 5G networks for optimizing performance and services often require large amounts of data, raising concerns about how this data is collected, stored, and processed [165], [166].
	Bias and Discrimination: Improper use of AI and ML can lead to biased outcomes, which can infringe on individuals' privacy and lead to discriminatory practices [167].
Edge Computing	*Local Data Processing:* Edge computing involves processing data closer to where it is generated, reducing latency [168]. However, it also means sensitive data [169] is processed and stored at multiple locations, increasing the risk of unauthorized access.
	Data Sovereignty: Ensuring data remains within legal jurisdictions and complies with local privacy laws when processed at the edge is a significant challenge [170].
Regulatory and Compliance Issues	*Diverse Regulations:* Navigating the diverse landscape of privacy regulations across different countries and regions is complex and challenging for global 5G networks [171].
	Enforcement: Ensuring compliance with privacy laws and regulations, and enforcing these standards across the vast 5G infrastructure, is a formidable task [172].

Evidently, the advent of 5G networks introduces numerous privacy challenges that require a comprehensive and proactive approach. By addressing these issues through robust security measures, privacy-by-design principles, and regulatory compliance, stakeholders can help ensure that the benefits of 5G are realized while safeguarding user privacy.

6. Performance issues in 5G networks

Realizing the full potential of 5G networks requires overcoming various performance-related challenges. Addressing these performance issues is paramount for ensuring optimal network functionality and delivering the anticipated benefits to users and industries [173]. Performance problems such as inconsistent latency, limited coverage, spectrum allocation difficulties, and interference can impede the effective deployment and operation of 5G networks [174]. Therefore, a comprehensive understanding of these issues and the development of robust solutions are essential to harness the capabilities of 5G and facilitate its widespread adoption and success. 5G networks represent a significant leap in performance compared to previous generations of cellular technology. One of the primary enhancements is speed; 5G can deliver data rates up to 10 Gbps, which is up to 100 times faster than 4G LTE. This remarkable speed improvement facilitates the seamless streaming of high-definition video, rapid downloading of large files, and enhanced user experiences in applications such as virtual reality (VR) and augmented reality (AR). Moreover, 5G networks boast significantly lower latency, often reduced to just 1 millisecond, which is crucial for real-time applications like autonomous driving, remote surgery, and interactive gaming. These advancements are underpinned by the deployment of new technologies, such as millimeter waves (mmWave), massive MIMO (Multiple Input Multiple Output), and beam-forming, which collectively enhance capacity, coverage, and spectral efficiency.

Beyond speed and latency, 5G networks also excel in handling a massive number of connected devices. This capability is essential for the Internet of Things (IoT), where billions of devices, from smart home gadgets to industrial sensors, require reliable connectivity. 5G's architecture is designed to support up to 1 million devices per square kilometer, ensuring robust performance even in densely populated areas. Additionally, 5G introduces network slicing, which allows operators to create multiple virtual networks within a single physical 5G infrastructure, each optimized for specific use cases and performance requirements. This flexibility is critical for supporting diverse applications, from consumer mobile services to industrial automation and smart city solutions. Overall, 5G networks are poised to revolutionize various sectors by providing unprecedented speed, low latency, and the capacity to support a vast number of connected devices. Figure 8 shows some of the key performance issues in 5G.

This section explores the key performance issues in 5G networks, examining the factors that affect network performance. By addressing these issues, we can ensure that 5G networks achieve their full potential, providing reliable, high-quality service [175] to users and supporting the myriad of applications that rely on this advanced technology.

Figure 8 Key Performance issues in 5G

5G networks promise significant improvements in speed, latency, capacity, and connectivity, but they also face various performance challenges. Table 5 presents an extensive discussion of the performance issues in 5G networks.

Table 5 Performance setbacks in 5G networks

Performance setback	**Details**
Spectrum Availability and Management	*Spectrum Allocation:* The availability of sufficient and appropriate spectrum is crucial for 5G performance [175]. Limited spectrum can lead to congestion and reduced network performance.
	Spectrum Fragmentation: 5G operates across various frequency bands (low, mid, and high) [177]. Managing and integrating these fragmented spectrums to ensure seamless performance is complex.
Signal Interference and Propagation	*High-Frequency Bands*: 5G utilizes high-frequency millimeter waves (mmWave) that offer higher bandwidth but are more susceptible to signal attenuation and interference [178], especially in urban environments with buildings and other obstacles.
	Propagation Loss: The higher frequency bands used in 5G have shorter wavelengths, leading to higher propagation losses and reduced coverage areas compared to lower frequency bands [179].
Network Infrastructure	*Dense Network Deployment:* Achieving the high-speed, low-latency performance promised by 5G requires dense deployment of small cells, which is costly and logistically challenging [180].
	Backhaul Capacity: Ensuring sufficient backhaul capacity to handle the increased data traffic generated by 5G networks is essential. Insufficient backhaul can lead to bottlenecks [181] and performance degradation.

Latency Issues	*Edge Computing:* To achieve ultra-low latency, 5G networks rely on edge computing to process data closer to the source. However, deploying and managing edge computing infrastructure effectively is challenging [182].
	Network Slicing: Implementing network slicing to allocate resources dynamically for different use cases (e.g., autonomous vehicles, remote surgery) requires sophisticated orchestration and can introduce latency if not managed properly [183].
Energy Efficiency	*Power Consumption:* The dense network of small cells and the need for constant connectivity in 5G networks increase power consumption [184], impacting both operational costs and environmental sustainability.
	Device Battery Life: Devices connected to 5G networks may experience reduced battery life due to higher power requirements for maintaining faster and more consistent connections [185].
Interoperability and Legacy Systems	*Integration with 4G and Older Networks:* Ensuring seamless interoperability with existing 4G and older networks is essential for a smooth transition to 5G [186]. Compatibility issues can lead to performance degradation.
	Handover Performance: Maintaining consistent performance during handovers [187] between 4G and 5G networks, as well as between different 5G cells, is critical to avoid service interruptions and latency spikes.
Quality of Service (QoS)	*Service Differentiation:* 5G networks must support a wide range of applications with varying QoS requirements [188]. Ensuring consistent performance across diverse use cases (e.g., high-speed internet, IoT, critical communications) is challenging.
	Resource Allocation: Dynamic resource allocation to meet the QoS demands of different applications requires sophisticated network management and can impact overall network performance [189].
Scalability	*Network Expansion:* Scaling 5G networks to accommodate the expected growth in connected devices and data traffic without compromising performance is a significant challenge [190].
	Management Complexity: As the network scales, managing and optimizing performance across a larger and more complex infrastructure becomes increasingly difficult [191].
Security Considerations	*Security Overheads:* Implementing robust security measures to protect against cyber threats can introduce latency and processing overheads, impacting network performance [192], [193].
	Attack Resilience: Ensuring the network remains resilient and performs well under potential security attacks, such as distributed denial of service (DDoS) attacks [194], is essential for maintaining performance.
Economic and Regulatory Factors	*Investment Costs:* The high costs associated with deploying and maintaining 5G infrastructure can impact the speed and extent of network rollouts, affecting overall performance [195].
	Regulatory Compliance: Navigating and complying with regulatory requirements in different regions can introduce delays and complexities in network deployment and performance optimization [196].

While 5G networks offer transformative benefits, they also present significant performance challenges that must be addressed through advanced technologies, strategic planning, and robust management practices. By tackling these issues proactively, stakeholders can ensure that 5G networks deliver on their promises of enhanced speed, capacity, and connectivity while maintaining optimal performance.

7. Discussion

The analysis of security, privacy, and performance issues in 5G networks reveals significant challenges that need to be addressed to realize the full potential of 5G technology. Our findings indicate that while 5G offers substantial advancements in speed, capacity, and connectivity, it also introduces new vulnerabilities and complexities that necessitate comprehensive solutions.

In the following sections, we discuss potential solutions to these identified issues, focusing on security, privacy, and performance in 5G networks. These solutions aim to enhance the robustness, privacy, and efficiency of 5G networks, ensuring they meet the demands of modern digital applications and services.

7.1. Solutions to security issues in 5G networks

Security issues in 5G networks stem from the increased attack surface due to the higher number of connected devices and the complexity of the network architecture. The findings highlight the prevalence of threats such as data breaches, unauthorized access, and network attacks that can compromise the integrity and confidentiality of data. Additionally, the integration of Internet of Things (IoT) devices, which often have limited security capabilities, further exacerbates these security risks. Security issues in 5G networks are multifaceted and require a comprehensive approach to address effectively [197], [198]. One fundamental solution is the implementation of advanced encryption protocols to ensure data confidentiality and integrity. Encrypting data both at rest and in transit prevents unauthorized access and tampering [199]. Additionally, the adoption of end-to-end encryption (E2EE) can further enhance security by ensuring that data remains encrypted throughout its entire journey from sender to recipient.

Another critical solution involves strengthening authentication mechanisms. Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide multiple forms of verification before accessing the network [200], [201]. This reduces the likelihood of unauthorized access, even if one form of authentication is compromised. Network slicing, a feature unique to 5G, can also enhance security by allowing operators to create isolated virtual networks for different applications [202], thus containing potential breaches and limiting their impact. Regular security audits and continuous monitoring are essential to identify and mitigate vulnerabilities promptly [203], [204]. Employing advanced threat detection systems that utilize artificial intelligence (AI) and machine learning (ML) [205] can help detect anomalies and potential security threats in real-time. These systems can analyze vast amounts of data to identify patterns and predict potential attacks, enabling proactive defense measures. Therefore, addressing security issues in 5G networks requires a comprehensive approach that encompasses technological, procedural, and policy-based measures. Table 6 discusses some of solutions to the security challenges in 5G networks.

Table 6 Solutions to the security challenges in 5G networks

Solution	Details
Advanced Encryption Techniques	*End-to-End Encryption:* Implementing robust end-to-end encryption for all data transmitted over 5G networks ensures that even if the data is intercepted, it cannot be read by unauthorized parties [206].
	Quantum-Resistant Encryption: With the advent of quantum computing, traditional encryption methods may become vulnerable [207]-[209]. Developing and deploying quantum-resistant encryption algorithms will future-proof 5G networks.
Secure Authentication and Identity Management	*Multi-Factor Authentication (MFA):* Utilizing MFA ensures that users and devices are authenticated through multiple verification methods, reducing the risk of unauthorized access [210], [211].
	Zero Trust Architecture: Implementing a zero trust security model where no user or device is trusted by default, even if inside the network perimeter [212]. Continuous verification is enforced.
	Secure Identity Management: Developing robust identity management systems that can securely manage identities and access rights for users and devices across the network [213].
Network Slicing Security	*Isolation Mechanisms:* Implementing strict isolation mechanisms to ensure that each network slice operates independently, preventing vulnerabilities in one slice from affecting others [214].
	Dynamic Security Policies: Applying dynamic and context-aware security policies for each network slice based on its specific requirements and threat landscape [215].
SDN and NFV security	*Secure SDN Controllers:* Protecting SDN controllers with robust security measures as they centralize control over network functions [216], making them prime targets for attacks.
	Virtualization Security: Ensuring that virtualized network functions (VNFs) are securely isolated and monitored to prevent lateral movement of threats within the virtual environment [217].

Supply Chain Security	*Vendor Vetting:* Conducting thorough vetting and risk assessments of all suppliers and vendors to ensure the integrity [218] of the hardware and software components used in the network.
	Secure Manufacturing Processes: Implementing secure manufacturing processes and continuous monitoring to detect and mitigate any attempts to compromise the supply chain [219].
Advanced Threat Detection and Response	*AI and ML:* Leveraging AI and ML for real-time threat detection and response [220]. These technologies can analyze vast amounts of data to identify and mitigate threats quickly.
	Anomaly Detection: Implementing advanced anomaly detection systems that can identify unusual patterns of behavior indicative of potential security threats [221].
Robust Incident Response and Recovery	*Incident Response Plans:* Developing and regularly updating comprehensive incident response plans to ensure rapid and effective action in the event of a security breach [222].
	Disaster Recovery and Business Continuity: Ensuring that robust disaster recovery and business continuity plans are in place to minimize downtime and data loss following a security incident [223], [224].
Regulatory Compliance and Standards	*Adhering to Standards:* Ensuring compliance with international and local security standards and regulations, such as the General Data Protection Regulation (GDPR) and National Institute of Standards and Technology (NIST) guidelines [225].
	Continuous Auditing: Conducting regular security audits and assessments to ensure ongoing compliance and to identify and address vulnerabilities [226].
Security by Design	*Integrating Security:* Embedding security considerations into the design and development of 5G infrastructure and applications from the outset [227].
	Secure Development Practices: Adopting secure software development practices, including regular code reviews, security testing, and vulnerability assessments [228].
Physical Security	*Securing Physical Assets:* Ensuring that physical infrastructure, such as base stations and data centers, are protected against tampering, theft, and other physical threats [229].
	Monitoring and Surveillance: Implementing robust monitoring and surveillance systems to detect and respond to physical security threats [230], [231].
Advanced Monitoring and Logging	*Continuous Monitoring:* Implementing continuous monitoring systems to keep track of all network activities and detect any suspicious behavior in real-time [232].
	Comprehensive Logging: Ensuring that all network activities are logged and that these logs are securely stored and regularly reviewed to detect and analyze security incidents [233].

Curbing security issues in 5G networks requires a multi-layered approach that combines advanced technologies, stringent policies, and continuous vigilance. By implementing robust security measures, fostering collaboration, and promoting a culture of security awareness, stakeholders can mitigate the risks associated with 5G networks and ensure a secure and resilient network environment.

7.2. Solutions to privacy issues in 5G networks

Privacy concerns in 5G networks are primarily related to the protection of user data and identity. The enhanced capabilities of 5G networks to collect and process granular location data raise significant privacy risks, including unauthorized tracking and profiling of users. The study underscores the need for robust privacy measures to safeguard sensitive user information from interception and misuse by malicious actors.

Addressing privacy issues in 5G networks necessitates a combination of technical and regulatory measures. One of the primary technical solutions is the implementation of dynamic pseudonymization techniques [234]. By regularly changing user identifiers, pseudonymization makes it difficult for attackers to track and profile users, thus enhancing privacy. Additionally, encryption plays a vital role in protecting user data and communications from interception and unauthorized access.

Privacy-preserving data analytics is another crucial area of focus. Techniques such as homomorphic encryption allow data to be analyzed in an encrypted form, ensuring that sensitive information remains protected throughout the analytical process [235]. Federated learning, which enables decentralized data analysis, also helps maintain privacy by keeping data local to the user's device while only sharing aggregated results.

Regulatory measures are equally important in protecting user privacy [236]. Compliance with data protection regulations such as the General Data Protection Regulation (GDPR) ensures that personal data is handled with the highest standards of privacy and security. Implementing privacy by design principles, where privacy considerations are integrated into the design and development of 5G technologies, can also help address privacy concerns from the outset. Evidently, addressing privacy issues in 5G networks requires a multifaceted approach, integrating technological, regulatory, and procedural measures. Table 7 discusses some of the most common solutions to privacy challenges in 5G networks.

Table 7 Solutions to privacy challenges in 5G networks

Solution	**Details**
Data Encryption	*End-to-End Encryption:* Implementing strong end-to-end encryption for all data transmitted over 5G networks ensures that data remains private and secure from source to destination [237].
	Advanced Encryption Standards: Using advanced encryption standards (AES) and developing quantum-resistant encryption methods [238] to protect data against current and future threats.
Privacy by Design	*Integrating Privacy Early:* Incorporating privacy considerations into the design and development of 5G infrastructure and services from the outset [239].
	Secure Development Practices: Employing secure software development practices, including privacy impact assessments, to identify and mitigate privacy risks early in the development process [240].
Secure Data Storage and Transmission	*Encryption at Rest:* Ensuring that all stored data, whether in local devices or cloud storage, is encrypted to protect against unauthorized access [241].
	Secure Communication Protocols: Using secure communication protocols (e.g., TLS, HTTPS) to protect data in transit [242].
Edge Computing Privacy	*Local Data Processing:* Utilizing edge computing to process data locally, reducing the need to transmit sensitive data over the network and minimizing the risk of interception [243], [244].
	Secure Edge Devices: Ensuring that edge devices are equipped with robust security measures [245] to protect data processed and stored at the edge.
Privacy-Preserving Technologies	*Differential Privacy:* Implementing differential privacy techniques [246] to allow data analysis while protecting individual privacy by adding statistical noise to the data.
	Homomorphic Encryption: Using homomorphic encryption [247] to enable data processing and analysis without exposing the raw data, thereby preserving privacy.
Regulatory Compliance	*Adherence to Regulations:* Ensuring compliance with data protection regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other relevant privacy laws [248].
	Regular Audits: Conducting regular privacy audits and assessments to ensure ongoing compliance with regulatory requirements and identify potential privacy risks [249].
Interoperability and Data Portability	*Interoperable Systems:* Designing 5G systems to be interoperable with other networks and systems while ensuring data privacy [250], [251].
	Data Portability: Allowing users to easily transfer their data between different service providers, giving them more control over their personal information [252].
	Continuous Monitoring: Implementing continuous monitoring systems to detect and respond to privacy breaches in real-time [253].

Advanced Monitoring and Logging	*Comprehensive Logging:* Ensuring that all network activities are logged securely and that these logs are regularly reviewed to detect and analyze potential privacy incidents [254].
Technology Innovation	*AI and ML for Privacy:* Leveraging artificial intelligence (AI) and machine learning (ML) [255], [256] to develop innovative privacy-preserving technologies and solutions.
	Blockchain for Privacy: Exploring the use of blockchain technology to enhance data security and privacy through decentralized and immutable ledgers [257].

Mitigating privacy issues in 5G networks requires a holistic approach that combines technological innovations, regulatory compliance, and robust privacy practices. By implementing these solutions, stakeholders can protect user privacy, build trust, and ensure the successful deployment and adoption of 5G technologies.

7.3. Solutions to performance issues in 5G networks

Performance issues in 5G networks are associated with the demand for low latency, high throughput, and reliable connectivity. The findings reveal that network congestion, inefficient spectrum utilization, and inadequate infrastructure can lead to performance degradation, impacting the user experience. Ensuring optimal performance in 5G networks requires addressing these challenges through strategic infrastructure deployment, effective spectrum management, and advanced traffic management techniques. Performance issues in 5G networks can significantly impact user experience and network efficiency. One of the key solutions to address these issues is the optimization of network infrastructure [258]. Deploying more small cells and enhancing network densification can improve coverage and capacity, reducing latency and increasing throughput. These small cells can be strategically placed in high-demand areas to ensure consistent performance.

Spectrum management is another critical aspect of improving 5G network performance. Efficient allocation and utilization of available spectrum resources can help mitigate congestion and interference [259]. Implementing dynamic spectrum sharing techniques allows operators to use spectrum more flexibly and efficiently, adapting to varying demand patterns in real-time. Advanced traffic management techniques can also enhance network performance [260]. Quality of Service (QoS) mechanisms prioritize critical applications and services, ensuring they receive the necessary bandwidth and low latency required for optimal performance. Additionally, network slicing can be employed to create dedicated virtual networks for different types of services [261], ensuring that performance-critical applications are not impacted by less demanding ones. It is clear that solving performance issues in 5G networks requires a multi-layered approach that integrates advanced technologies, strategic planning, and efficient management. Table 8 gives a description of the most promising solutions to performance challenges in 5G networks.

Table 8 Solutions to performance challenges in 5G networks

Solution	**Details**
Spectrum Management and Allocation	*Dynamic Spectrum Sharing:* Utilizing dynamic spectrum sharing techniques to optimize the use of available spectrum [262]. This approach allows 5G networks to coexist with existing 4G and other wireless networks, improving spectrum efficiency.
	Spectrum Reallocation: Governments and regulatory bodies can reallocate spectrum bands to ensure that 5G networks have access to sufficient and appropriate frequencies, including low, mid, and high bands [263].
	Carrier Aggregation: Combining multiple spectrum bands to increase bandwidth and improve network performance, providing higher data rates and better coverage [264].
Advanced Antenna Technologies	*Massive MIMO (Multiple Input, Multiple Output)*: Implementing Massive MIMO technology [265], which uses a large number of antennas to improve spectral efficiency, enhance capacity, and provide better coverage.
	Beamforming: Utilizing beamforming techniques to direct signals to specific users, reducing interference, and increasing the efficiency and reliability [266] of data transmission.

Dense Network Deployment	*Small Cells:* Deploying a dense network of small cells to improve coverage and capacity, especially in urban areas and high-traffic locations [267]. Small cells help offload traffic from macro cells, reducing congestion.
	Heterogeneous Networks (HetNets): Integrating different types of cells, such as macro cells, small cells, and Wi-Fi hotspots, to create a heterogeneous network that optimizes coverage and capacity [268].
Efficient Backhaul and Fronthaul Solutions	*High-Capacity Backhaul:* Ensuring high-capacity backhaul connections, such as fiber optics, to handle the increased data traffic generated by 5G networks [269]. Microwave and millimeter-wave links can also be used where fiber deployment is challenging.
	Fronthaul Optimization: Optimizing fronthaul connections between remote radio heads (RRHs) and baseband units (BBUs) to reduce latency and improve data throughput [270].
Edge Computing	*Multi-Access Edge Computing (MEC):* Deploying MEC to process data closer to the source, reducing latency and improving response times for real-time applications such as autonomous vehicles and industrial automation [271], [272].
	Distributed Computing Resources: Implementing distributed computing resources at the network edge to handle localized data processing [273], reducing the burden on centralized data centers.
Network Slicing	*Dynamic Network Slicing:* Implementing dynamic network slicing to create virtual networks tailored to specific use cases and performance requirements [274]. Each slice can be optimized for different applications, such as IoT, ultra-reliable low-latency communications (URLLC), or enhanced mobile broadband (eMBB).
	Slice Orchestration: Utilizing advanced orchestration tools to manage and optimize network slices dynamically [275], ensuring efficient resource allocation and performance.
AI and ML	*Predictive Analytics*: Leveraging AI and ML for predictive analytics to anticipate network demands and optimize resource allocation proactively [276].
	Network Optimization: Using AI and ML algorithms to optimize network performance [277] in real-time, including traffic management, interference mitigation, and load balancing.
QoS Management	*Prioritization of Traffic:* Implementing QoS mechanisms to prioritize traffic based on application requirements [278], ensuring that critical services receive the necessary bandwidth and low latency.
	Resource Allocation: Dynamically allocating network resources to meet the specific QoS requirements of different applications and services [280].
Interference Management	*Advanced Interference Mitigation*: Utilizing advanced interference mitigation techniques [280], such as coordinated multipoint (CoMP) and interference cancellation, to reduce signal interference and improve performance.
	Spectrum Monitoring: Continuously monitoring the spectrum for interference and adjusting network parameters dynamically to mitigate its impact [281].
Security and Reliability	*Robust Security Measures*: Implementing strong security measures to protect the network from cyber threats [282], ensuring reliable and uninterrupted service.
	Redundancy and Failover: Designing network infrastructure with redundancy and failover mechanisms [283] to maintain performance during outages or failures.
User Equipment (UE) Optimization	*Advanced Modulation Techniques*: Using advanced modulation and coding schemes to improve data rates and spectral efficiency [284].
	Device Optimization: Ensuring that user devices are optimized for 5G performance [285], including support for the latest standards and efficient power management.

The effective mitigation of performance issues in 5G networks requires a comprehensive and coordinated effort across multiple domains, including technology, infrastructure, policy, and regulation. By implementing these solutions, stakeholders can overcome the challenges associated with 5G deployment and ensure that networks deliver the high-speed, low-latency, and high-capacity performance promised by this next-generation technology.

8. Research gaps

While this study identifies critical issues in 5G network security, privacy, and performance, several research gaps remain that warrant further investigation:

- *Holistic Security Frameworks*: Existing research primarily addresses individual security measures, but there is a lack of comprehensive frameworks that integrate various security protocols and techniques into a unified, holistic approach [286]. Future research should focus on developing and validating such frameworks to ensure end-to-end security in 5G networks.
- *Dynamic Privacy Protection Mechanisms*: Current privacy protection methods, such as pseudonymization and encryption [287], need to be adapted dynamically to respond to evolving threats and user contexts. Research is needed to develop adaptive privacy mechanisms that can provide real-time protection without compromising network performance.
- *Scalability of Security Solutions*: As the number of connected devices in 5G networks continues to grow, ensuring that security solutions can scale effectively is a significant challenge. There is a need for scalable security architectures [288] that can maintain high levels of protection across millions of devices without causing performance bottlenecks.
- *Performance Optimization in Diverse Environments*: While performance optimization techniques [289] exist, there is a gap in understanding how these methods perform in diverse real-world environments with varying levels of infrastructure and user density. Research should explore the effectiveness of different optimization strategies across various scenarios to develop more universally applicable solutions.
- *Impact of Emerging Technologies*: Technologies such as artificial intelligence (AI), machine learning (ML), and edge computing have the potential to enhance 5G networks significantly. However, their impact on security, privacy, and performance [290] is not fully understood. Future studies should investigate how these emerging technologies can be integrated into 5G networks to improve overall efficiency and security.
- *User-Centric Privacy Solutions*: Much of the current research focuses on network-level privacy protections [291], but there is a gap in user-centric solutions that empower individuals to control their own data privacy. Developing tools and frameworks that give users greater control over their data in 5G networks is an important area for future research.

9. Future research scopes

The rapid evolution of 5G technology presents numerous opportunities for further research, particularly in the areas of security, privacy, and performance. As 5G continues to develop and become more widespread, addressing its associated challenges and leveraging its potential will require ongoing investigation. This section outlines several future research scopes that are crucial for advancing the understanding and implementation of 5G networks.

Future research should focus on developing advanced security frameworks to address the unique challenges posed by 5G networks. Key areas include the integration of artificial intelligence (AI) and machine learning (ML) to enhance threat detection and mitigation in real-time [292]. AI and ML can identify patterns, predict attacks, and automate security processes, reducing human intervention. Another essential area is quantum-safe cryptography [293], ensuring that 5G networks remain secure against future threats from quantum computing. Additionally, exploring blockchain technology can enhance security by providing decentralized, tamper-proof ledgers for secure transactions and data integrity.

Privacy concerns in 5G networks require innovative solutions that protect user data while maintaining network performance. Future research should focus on privacy-preserving data analytics techniques, such as homomorphic encryption [294] and federated learning, which allow data processing without exposing sensitive information. User-controlled privacy settings are also important, empowering individuals to manage their data privacy through interfaces and protocols. Additionally, research into implementing privacy by design principles [295] and regulatory compliance within 5G technologies is essential, ensuring privacy considerations are integrated from design to deployment.

As demand for high-performance 5G networks grows, future research should optimize network performance to meet diverse user needs. Key areas include dynamic network resource allocation methods [296] to optimize performance based on real-time demand and conditions, and edge computing to enhance network efficiency and reduce latency by bringing computation and storage closer to the end-user [297]. Additionally, improving the energy efficiency of 5G networks is crucial, addressing the environmental impact of increased infrastructure through sustainable practices and technologies.

The complexity of 5G networks necessitates interdisciplinary research that combines insights from various fields, including computer science, telecommunications, cybersecurity, and data science. Future research should foster cross-domain collaboration between academia, industry, and government to address the multifaceted challenges of 5G. Socio-technical studies examining the social and technical implications of 5G deployment are essential, including user behavior, adoption barriers, and societal impact. Moreover, developing effective policies and governance frameworks that support the secure, private, and efficient deployment of 5G networks is critical, addressing regulatory challenges and ensuring policies keep pace with technological advancements.

10. Conclusion

The exploration of 5G networks uncovers a multifaceted landscape where advancements in technology bring both opportunities and challenges. This study has delved into the critical issues of security, privacy, and performance within 5G networks, highlighting the urgent need for innovative solutions and ongoing research. In the realm of security, the dynamic and complex nature of 5G infrastructure necessitates advanced frameworks and methodologies. The integration of AI and ML for real-time threat detection and response, along with quantum-safe cryptography and blockchain technologies, presents promising avenues for fortifying 5G networks against emerging threats. Privacy remains a cornerstone of user trust and regulatory compliance. Developing privacy-preserving data analytics, user-controlled privacy settings, and embedding privacy by design principles into 5G technologies are vital steps towards ensuring that user data is protected without compromising network performance. Performance optimization is critical as the demand for high-speed, reliable 5G connectivity grows. Dynamic resource allocation, edge computing, and energy-efficient technologies are essential for maximizing network efficiency, reducing latency, and addressing environmental sustainability. Interdisciplinary research and cross-domain collaboration are pivotal in addressing the comprehensive challenges posed by 5G. By combining insights from various fields and fostering partnerships between academia, industry, and government, a holistic approach to 5G development can be achieved. Socio-technical studies and effective policy frameworks will ensure that 5G deployment is not only technically robust but also socially and economically beneficial. In summary, this study underscores the importance of continued research and innovation in advancing the security, privacy, and performance of 5G networks. As we look to the future, embracing interdisciplinary approaches and fostering collaborative efforts will be key to unlocking the full potential of 5G technology, ensuring it serves as a foundation for the next generation of digital connectivity.

References

[1] Guo J, Wang L, Zhou W, Wei C. Powering green digitalization: evidence from 5G network infrastructure in China. Resources, Conservation and Recycling. 2022 Jul 1, 182:106286.

[2] Shin H, Jung J, Koo Y. Forecasting the video data traffic of 5 G services in south korea. Technological Forecasting and Social Change. 2020 Apr 1, 153:119948.

[3] Liu G, Jiang D. 5G: Vision and requirements for mobile communication system towards year 2020. Chinese Journal of Engineering. 2016, 2016(1):5974586.

[4] Attaran M. The impact of 5G on the evolution of intelligent automation and industry digitization. Journal of ambient intelligence and humanized computing. 2023 May, 14(5):5977-93.

[5] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[6] Patel B, Yarlagadda VK, Dhameliya N, Mullangi K, Vennapusa SC. Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering. Engineering International. 2022, 10(2):117-30.

[7] Longo F, Padovano A, Aiello G, Fusto C, Certa A. How 5G-based industrial IoT is transforming human-centered smart factories: A Quality of Experience model for Operator 4.0 applications. IFAC-PapersOnLine. 2021 Jan 1, 54(1):255-62.

[8] Al-Turjman F. 5G-Enabled Devices and Smart Spaces in Social-IoT. InSmart Things and Femtocells 2018 Jul 3 (pp. 137-166). CRC Press.

[9] Rao SK, Prasad R. Impact of 5G technologies on industry 4.0. Wireless personal communications. 2018 May, 100:145-59.

[10] Goyal P, Sahoo AK. A roadmap towards connected living: 5G mobile technology. Int. J. Innov. Technol. Explor. Eng. 2019, 9(1):1670-85.

[11] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[12] Narayanan A, Ramadan E, Carpenter J, Liu Q, Liu Y, Qian F, Zhang ZL. A first look at commercial 5G performance on smartphones. InProceedings of The Web Conference 2020 2020 Apr 20 (pp. 894-905).

[13] Javaid N, Sher A, Nasir H, Guizani N. Intelligence in IoT-based 5G networks: Opportunities and challenges. IEEE Communications Magazine. 2018 Oct 16, 56(10):94-100.

[14] Shafique K, Khawaja BA, Sabir F, Qazi S, Mustaqim M. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. Ieee Access. 2020 Jan 28, 8:23022-40.

[15] Le NT, Hossain MA, Islam A, Kim DY, Choi YJ, Jang YM. Survey of promising technologies for 5G networks. Mobile information systems. 2016, 2016(1):2676589.

[16] Rahimi H, Zibaeenejad A, Safavi AA. A novel IoT architecture based on 5G-IoT and next generation technologies. In2018 IEEE 9th annual information technology, electronics and mobile communication conference (IEMCON) 2018 Nov 1 (pp. 81-88). IEEE.

[17] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[18] Ford R, Zhang M, Mezzavilla M, Dutta S, Rangan S, Zorzi M. Achieving ultra-low latency in 5G millimeter wave cellular networks. IEEE Communications Magazine. 2017 Mar 13, 55(3):196-203.

[19] Nadir Z, Taleb T, Flinck H, Bouachir O, Bagaa M. Immersive services over 5G and beyond mobile systems. IEEE Network. 2021 Nov 2, 35(6):299-306.

[20] Kusuma HM, Shukla VK, Gupta S. Enabling VR/AR and tactile through 5G network. In2021 International Conference on Communication Information and Computing Technology (ICCICT) 2021 Jun 25 (pp. 1-6). IEEE.

[21] Orlosky J, Kiyokawa K, Takemura H. Virtual and augmented reality on the 5G highway. Journal of Information Processing. 2017, 25:133-41.

[22] Silva MM, Guerreiro J. On the 5G and Beyond. Applied Sciences. 2020 Oct 12, 10(20):7091.

[23] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[24] Ahad A, Tahir M, Aman Sheikh M, Ahmed KI, Mughees A, Numani A. Technologies trend towards 5G network for smart health-care using IoT: A review. Sensors. 2020 Jul 21, 20(14):4047.

[25] Khanh QV, Hoai NV, Manh LD, Le AN, Jeon G. Wireless communication technologies for IoT in 5G: Vision, applications, and challenges. Wireless Communications and Mobile Computing. 2022, 2022(1):3229294.

[26] Cheng J, Chen W, Tao F, Lin CL. Industrial IoT in 5G environment towards smart manufacturing. Journal of Industrial Information Integration. 2018 Jun 1, 10:10-9.

[27] Subedi P, Alsadoon A, Prasad PW, Rehman S, Giweli N, Imran M, Arif S. Network slicing: A next generation 5G perspective. EURASIP Journal on Wireless Communications and Networking. 2021 Apr 23, 2021(1):102.

[28] Zhang S. An overview of network slicing for 5G. IEEE Wireless Communications. 2019 Apr 11, 26(3):111-7.

[29] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[30] Minoli D, Occhiogrosso B. Practical aspects for the integration of 5G networks and IoT applications in smart cities environments. Wireless Communications and Mobile Computing. 2019, 2019(1):5710834.

[31] Mukherjee S, Gupta S, Rawlley O, Jain S. Leveraging big data analytics in 5G-enabled IoT and industrial IoT for the development of sustainable smart cities. Transactions on Emerging Telecommunications Technologies. 2022 Dec, 33(12):e4618.

[32] Varga P, Peto J, Franko A, Balla D, Haja D, Janky F, Soos G, Ficzere D, Maliosz M, Toka L. 5G support for industrial IoT applications—challenges, solutions, and research gaps. Sensors. 2020 Feb 4, 20(3):828.

[33] Kumhar M, Bhatia J. Emerging communication technologies for 5G-Enabled internet of things applications. Blockchain for 5G-Enabled IoT: The new wave for Industrial Automation. 2021:133-58.

[34] Rao SK, Prasad R. Impact of 5G technologies on smart city implementation. Wireless Personal Communications. 2018 May, 100:161-76.

[35] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[36] Ezema ME, Okoye FA, Okwori AO. A framework of 5G networks as the foundation for IoTs technology for improved future network. International Journal of the Physical Sciences. 2019, 14(10):97-107.

[37] Mistry I, Tanwar S, Tyagi S, Kumar N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical systems and signal processing. 2020 Jan 1, 135:106382.

[38] Jordaan CG, Malekian N, Malekian R. Internet of things and 5G solutions for development of smart cities and connected systems. Communications of the CCISA. 2019 May 1, 25(2):1-6.

[39] Shehab MJ, Kassem I, Kutty AA, Kucukvar M, Onat N, Khattab T. 5G networks towards smart and sustainable cities: A review of recent developments, applications and future perspectives. IEEE Access. 2021 Dec 30, 10:2987-3006.

[40] Painuly S, Sharma S, Matta P. Future trends and challenges in next generation smart application of 5G-IoT. In2021 5th international conference on computing methodologies and communication (ICCMC) 2021 Apr 8 (pp. 354-357). IEEE.

[41] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[42] Khan R, Kumar P, Jayakody DN, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials. 2019 Aug 8, 22(1):196-248.

[43] Porambage P, Gür G, Osorio DP, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society. 2021 May 10, 2:1094-122.

[44] Aswathy SU, Tyagi AK. Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future. InSecurity and Privacy-Preserving Techniques in Wireless Robotics 2022 Aug 17 (pp. 163-210). CRC Press.

[45] Demertzi V, Demertzis S, Demertzis K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences. 2023 Jan 6, 13(2):790.

[46] Zhang X, Yadollahi MM, Dadkhah S, Isah H, Le DP, Ghorbani AA. Data breach: analysis, countermeasures and challenges. International Journal of Information and Computer Security. 2022, 19(3-4):402-42.

[47] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[48] Guevara L, Auat Cheein F. The role of 5G technologies: Challenges in smart cities and intelligent transportation systems. Sustainability. 2020 Aug 11, 12(16):6469.

[49] Gohar A, Nencioni G. The role of 5G technologies in a smart city: The case for intelligent transportation system. Sustainability. 2021 May 6, 13(9):5188.

[50] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11, 12(6):1333.

[51] Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science. 2021 Mar 9, 3:563060.

[52] Vaishy S, Gupta H. Cybercriminals' Motivations for Targeting Government Organizations. In2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2021 Sep 3 (pp. 1-6). IEEE.

[53] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9, 8(2):20.

[54] Sicari S, Rizzardi A, Coen-Porisini A. 5G In the internet of things era: An overview on security and privacy challenges. Computer Networks. 2020 Oct 9, 179:107345.

[55] Liu S, Yan Z. Efficient privacy protection protocols for 5G-enabled positioning in industrial IoT. IEEE Internet of Things Journal. 2022 Mar 22, 9(19):18527-38.

[56] Sasiain J, Sanz A, Astorga J, Jacob E. Towards flexible integration of 5G and IIoT technologies in industry 4.0: A practical use case. Applied Sciences. 2020 Oct 29, 10(21):7670.

[57] Bega D, Gramaglia M, Bernardos Cano CJ, Banchs A, Costa-Perez X. Toward the network of the future: From enabling technologies to 5G concepts. Transactions on Emerging Telecommunications Technologies. 2017 Aug, 28(8):e3205.

[58] Singh SK, Singh R, Kumbhani B. The evolution of radio access network towards open-RAN: Challenges and opportunities. In2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) 2020 Apr 6 (pp. 1-6). IEEE.

[59] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[60] Tripathi S, Sabu NV, Gupta AK, Dhillon HS. Millimeter-wave and terahertz spectrum for 6G wireless. In6G Mobile Wireless Networks 2021 Mar 22 (pp. 83-121). Cham: Springer International Publishing.

[61] Benseny J, Lahteenmaki J, Toyli J, Hammainen H. Urban wireless traffic evolution: The role of new devices and the effect of policy. Telecommunications Policy. 2023 Aug 1, 47(7):102595.

[62] Oughton EJ, Lehr W, Katsaros K, Selinis I, Bubley D, Kusuma J. Revisiting wireless internet connectivity: 5G vs Wi-Fi 6. Telecommunications Policy. 2021 Jun 1, 45(5):102127.

[63] Habibi MA, Nasimi M, Han B, Schotten HD. A comprehensive survey of RAN architectures toward 5G mobile communication system. Ieee Access. 2019 May 28, 7:70371-421.

[64] Lee YL, Qin D, Wang LC, Sim GH. 6G massive radio access networks: Key applications, requirements and challenges. IEEE Open Journal of Vehicular Technology. 2020 Dec 15, 2:54-66.

[65] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[66] Li S, Da Xu L, Zhao S. 5G Internet of Things: A survey. Journal of Industrial Information Integration. 2018 Jun 1, 10:1-9.

[67] Akpakwu GA, Silva BJ, Hancke GP, Abu-Mahfouz AM. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE access. 2017 Dec 4, 6:3619-47.

[68] Abdulghaffar A, Mahmoud A, Abu-Amara M, Sheltami T. Modeling and evaluation of software defined networking based 5G core network architecture. IEEE Access. 2021 Jan 8, 9:10179-98.

[69] Ghosh A, Maeder A, Baker M, Chandramouli D. 5G evolution: A view on 5G cellular technology beyond 3GPP release 15. IEEE access. 2019 Sep 6, 7:127639-51.

[70] Saley AM, Ndiaye M, Niane K, Raimy A, Ba PN. Study and Evaluation of a hybrid architecture to optimize resources in the 5G core network. In2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET) 2022 Mar 3 (pp. 1-5). IEEE.

[71] Du K, Wang L, Zhu Z, Yan Y, Wen X. Converged Service-based Architecture for Next-Generation Mobile Communication Networks. In2023 IEEE Wireless Communications and Networking Conference (WCNC) 2023 Mar 26 (pp. 1-6). IEEE.

[72] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[73] Lake D, Wang N, Tafazolli R, Samuel L. Softwarization of 5G networks–implications to open platforms and standardizations. IEEE access. 2021 Apr 8, 9:88902-30.

[74] Neves P, Calé R, Costa M, Gaspar G, Alcaraz-Calero J, Wang Q, Nightingale J, Bernini G, Carrozzo G, Valdivieso Á, Villalba LJ. Future mode of operations for 5G–The SELFNET approach enabled by SDN/NFV. Computer Standards & Interfaces. 2017 Nov 1, 54:229-46.

[75] Zhang Y, Zhang ZL. Enhancing performance, security, and management in network function virtualization. In2020 IEEE conference on network function virtualization and software defined networks (NFV-SDN) 2020 Nov 10 (pp. 126-131). IEEE.

[76] Alvarez F, Breitgand D, Griffin D, Andriani P, Rizou S, Zioulis N, Moscatelli F, Serrano J, Keltsch M, Trakadas P, Phan TK. An edge-to-cloud virtualized multimedia service platform for 5G networks. IEEE Transactions on Broadcasting. 2019 Mar 13, 65(2):369-80.

[77] Quintana-Ramirez I, Tsiopoulos A, Lema MA, Sardis F, Sequeira L, Arias J, Raman A, Azam A, Dohler M. The making of 5g: Building an end-to-end 5g-enabled system. IEEE Communications Standards Magazine. 2018 Dec, 2(4):88-96.

[78] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[79] Babbar H, Rani S, AlZubi AA, Singh A, Nasser N, Ali A. Role of network slicing in software defined networking for 5G: Use cases and future directions. IEEE Wireless Communications. 2022 Feb, 29(1):112-8.

[80] Tadros CN, Mokhtar B, Rizk MR. Software defined network-based management architecture for 5g network. InParadigms of Smart and Intelligent Communication, 5G and Beyond 2023 May 24 (pp. 171-195). Singapore: Springer Nature Singapore.

[81] Cunha J, Ferreira P, Castro EM, Oliveira PC, Nicolau MJ, Núñez I, Sousa XR, Serôdio C. Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. Future Internet. 2024 Jun 27, 16(7):226.

[82] Deepa V, Sivakumar B. Software-defined Networking for IoT. InBlockchain and Digital Twin Enabled IoT Networks 2024 Jul 19 (pp. 165-181). CRC Press.

[83] Saxena S, Chandan RR, Krishnamoorthy R, Kumar U, Singh P, Pandey AK, Gupta SK. Original Research Article Transforming transportation: Embracing the potential of 5G, heterogeneous networks, and software defined networking in intelligent transportation systems. Journal of Autonomous Intelligence. 2024, 7(4).

[84] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[85] Botez R, Costa-Requena J, Ivanciu IA, Strautiu V, Dobrota V. SDN-based network slicing mechanism for a scalable 4G/5G core network: A kubernetes approach. Sensors. 2021 May 29, 21(11):3773.

[86] Ma L, Wen X, Wang L, Lu Z, Knopp R. An SDN/NFV based framework for management and deployment of service based 5G core network. China Communications. 2018 Oct 8, 15(10):86-98.

[87] Debbabi F, Jmal R, Chaari Fourati L. 5G network slicing: Fundamental concepts, architectures, algorithmics, projects practices, and open issues. Concurrency and Computation: Practice and Experience. 2021 Oct 25, 33(20):e6352.

[88] Shu Z, Taleb T. A novel QoS framework for network slicing in 5G and beyond networks based on SDN and NFV. IEEE Network. 2020 Apr 22, 34(3):256-63.

[89] Singh R, Mehbodniya A, Webber JL, Dadheech P, Pavithra G, Alzaidi MS, Akwafo R. Analysis of network slicing for management of 5G networks using machine learning techniques. Wireless Communications and Mobile Computing. 2022, 2022(1):9169568.

[90] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19, 14(12):1297.

[91] Fakhouri HN, Alawadi S, Awaysheh FM, Hani IB, Alkhalaileh M, Hamad F. A comprehensive study on the role of machine learning in 5G security: challenges, technologies, and solutions. Electronics. 2023 Nov 10, 12(22):4604.

[92] Kumar GE, Lydia M, Levron Y. Security challenges in 5G and IoT networks: A review. Secure Communication for 5G and IoT Networks. 2022:1-3.

[93] Boodai J, Alqahtani A, Frikha M. Review of Physical Layer Security in 5G Wireless Networks. Applied Sciences. 2023 Jun 19, 13(12):7277.

[94] Ahmad IA, Osasona F, Dawodu SO, Obi OC, Anyanwu AC, Onwusinkwue S. Emerging 5G technology: A review of its far-reaching implications for communication and security.

[95] Shukla V, Kushwaha M, Sharma R, Joshi HD. A Note on 5G Networks: Security Issues, Challenges and Connectivity Approaches. InInternational Conference on Cryptology & Network Security with Machine Learning 2023 Oct 27 (pp. 95-114). Singapore: Springer Nature Singapore.

[96] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[97] Thyagaturu AS, Shantharama P, Nasrallah A, Reisslein M. Operating systems and hypervisors for network functions: A survey of enabling technologies and research studies. IEEE Access. 2022 Jul 29, 10:79825-73.

[98] Scalise P, Boeding M, Hempel M, Sharif H, Delloiacovo J, Reed J. A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas. Future Internet. 2024 Feb 20, 16(3):67.

[99] Santos J, Wauters T, Volckaert B, De Turck F. Towards low-latency service delivery in a continuum of virtual resources: State-of-the-art and research directions. IEEE Communications Surveys & Tutorials. 2021 Jul 7, 23(4):2557-89.

[100] Giles K, Hartmann K. Emergence of 5G Networks and Implications for Cyber Conflict. In2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon) 2022 May 31 (Vol. 700, pp. 405-419). IEEE.

[101] Wang N, Wang P, Alipour-Fanid A, Jiao L, Zeng K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. IEEE internet of things journal. 2019 Jul 9, 6(5):8169-81.

[102] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[103] Narayanan A, De Sena AS, Gutierrez-Rojas D, Melgarejo DC, Hussain HM, Ullah M, Bayhan S, Nardelli PH. Key advances in pervasive edge computing for industrial Internet of Things in 5G and beyond. IEEE Access. 2020 Nov 12, 8:206734-54.

[104] Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials. 2018 Jul 12, 20(4):3453-95.

[105] Mohan JP, Sugunaraj N, Ranganathan P. Cyber security threats for 5G networks. In2022 IEEE international conference on electro information technology (eIT) 2022 May 19 (pp. 446-454). IEEE.

[106] Cruz D, Cruz T, Pereira V, Simões P. Designing a high-fidelity Testbed for 5G-based Industrial IoT. InProceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS 2023), Athens, Greece (June 2023). DOI 2023 Jun 22 (Vol. 10).

[107] Khuntia M, Singh D, Sahoo S. Impact of internet of things (IoT) on 5G. InIntelligent and Cloud Computing: Proceedings of ICICC 2019, Volume 2 2021 (pp. 125-136). Springer Singapore.

[108] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[109] Wazid M, Das AK, Shetty S, Gope P, Rodrigues JJ. Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap. IEEE Access. 2020 Dec 28, 9:4466-89.

[110] Gaba GS, Kumar G, Kim TH, Monga H, Kumar P. Secure device-to-device communications for 5g enabled internet of things applications. Computer Communications. 2021 Mar 1, 169:114-28.

[111] De Alwis C, Porambage P, Dev K, Gadekallu TR, Liyanage M. A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions. IEEE Communications Surveys & Tutorials. 2023 Sep 6.

[112] Wichary T, Mongay Batalla J, Mavromoustakis CX, Żurek J, Mastorakis G. Network slicing security controls and assurance for verticals. Electronics. 2022 Jan 11, 11(2):222.

[113] Hakak S, Gadekallu TR, Maddikunta PK, Ramu SP, Parimala M, De Alwis C, Liyanage M. Autonomous Vehicles in 5G and beyond: A Survey. Vehicular Communications. 2023 Feb 1, 39:100551.

[114] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[115] Muhammad T. Revolutionizing Network Control: Exploring the Landscape of Software-Defined Networking (SDN). International Journal of Computer Science and Technology. 2019, 3(1):36-68.

[116] Paliwal M, Shrimankar D, Tembhurne O. Controllers in SDN: A review report. IEEE access. 2018 Jun 11, 6:36256-70.

[117] Zhang T, Qiu H, Linguaglossa L, Cerroni W, Giaccone P. NFV platforms: Taxonomy, design choices and future challenges. IEEE Transactions on Network and Service Management. 2020 Dec 22, 18(1):30-48.

[118] Fei X, Liu F, Zhang Q, Jin H, Hu H. Paving the way for NFV acceleration: A taxonomy, survey and future directions. ACM Computing Surveys (CSUR). 2020 Aug 20, 53(4):1-42.

[119] Zimba A, Chen H, Wang Z, Chishimba M. Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. Future Generation Computer Systems. 2020 May 1, 106:501-17.

[120] Rejeb A, Keogh JG. 5G networks in the value chain. Wireless Personal Communications. 2021 Mar, 117(2):1577-99.

[121] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[122] Nandy T, Idris MY, Noor RM, Kiah LM, Lun LS, Juma'at NB, Ahmedy I, Ghani NA, Bhattacharyya S. Review on security of internet of things authentication mechanism. IEEE Access. 2019 Oct 16, 7:151054-89.

[123] Indu I, Anand PR, Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal. 2018 Aug 1, 21(4):574-88.

[124] Humayun M, Jhanjhi NZ, Alruwaili M, Amalathas SS, Balasubramanian V, Selvaraj B. Privacy protection and energy optimization for 5G-aided industrial Internet of Things. Ieee Access. 2020 Oct 6, 8:183665-77.

[125] Loghin D, Cai S, Chen G, Dinh TT, Fan F, Lin Q, Ng J, Ooi BC, Sun X, Ta QT, Wang W. The disruptions of 5G on data-driven technologies and applications. IEEE transactions on knowledge and data engineering. 2020 Jan 17, 32(6):1179-98.

[126] Trakadas P, Nomikos N, Michailidis ET, Zahariadis T, Facca FM, Breitgand D, Rizou S, Masip X, Gkonis P. Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues and relevant architecture. Sensors. 2019 Aug 17, 19(16):3591.

[127] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[128] Salahdine F, Han T, Zhang N. Security in 5G and beyond recent advances and future challenges. Security and Privacy. 2023 Jan, 6(1):e271.

[129] Lamssaggad A, Benamar N, Hafid AS, Msahli M. A survey on the current security landscape of intelligent transportation systems. IEEE Access. 2021 Jan 8, 9:9180-208.

[130] Abdel Hakeem SA, Hussein HH, Kim H. Security requirements and challenges of 6G technologies and applications. Sensors. 2022 Mar 2, 22(5):1969.

[131] Hussain R, Hussain F, Zeadally S. Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems. 2019 Dec 1, 101:843-64.

[132] Lehto M. Cyber-attacks against critical infrastructure. InCyber security: Critical infrastructure protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[133] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25, 19(4):e0301277.

[134] Jahankhani H, Kendzierskyj S, Hussien O. Approaches and Methods for Regulation of Security Risks in 5G and 6G. InWireless Networks: Cyber Security Threats and Countermeasures 2023 Aug 24 (pp. 43-70). Cham: Springer International Publishing.

[135] Ortiz J, Fernández PJ, Sanchez-Iborra R, Bernabe JB, Santa J, Skarmeta A. Enforcing GDPR regulation to vehicular 5G communications using edge virtual counterparts. In2020 IEEE 3rd 5G World Forum (5GWF) 2020 Sep 10 (pp. 121-126). IEEE.

[136] Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence. 2022 Dec 31, 36(1):2037254.

[137] Itodo C, Ozer M. Multivocal Literature Review on Zero-Trust Security Implementation. Computers & Security. 2024 Mar 29:103827.

[138] de Carné de Carnavalet X, van Oorschot PC. A Survey and Analysis of TLS Interception Mechanisms and Motivations: Exploring how end-to-end TLS is made "end-to-me" for web traffic. ACM Computing Surveys. 2023 Jul 13, 55(13s):1-40.

[139] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[140] Afaq A, Haider N, Baig MZ, Khan KS, Imran M, Razzak I. Machine learning for 5G security: Architecture, recent advances, and challenges. Ad Hoc Networks. 2021 Dec 1, 123:102667.

[141] Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences. 2021 May 17, 11(10):4580.

[142] Sullivan S, Brighente A, Kumar SA, Conti M. 5G security challenges and solutions: a review by OSI layers. Ieee Access. 2021 Aug 16, 9:116294-314.

[143] Suomalainen J, Julku J, Vehkaperä M, Posti H. Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions. IEEE Open Journal of the Communications Society. 2021 Jul 2, 2:1590-615.

[144] Wu Y, Ma Y, Dai HN, Wang H. Deep learning for privacy preservation in autonomous moving platforms enhanced 5G heterogeneous networks. Computer Networks. 2021 Feb 11, 185:107743.

[145] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3, 19(1):e0296469.

[146] Chettri L, Bera R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Internet of Things Journal. 2019 Oct 22, 7(1):16-32.

[147] Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, Ladid L. Internet of things in the 5G era: Enablers, architecture, and business models. IEEE journal on selected areas in communications. 2016 Feb 3, 34(3):510-27.

[148] Kröger JL, Miceli M, Müller F. How data can be used against people: A classification of personal data misuses. Available at SSRN 3887097. 2021 Dec 30.

[149] Iavich M, Akhalaia G, Bocu R. Device Tracking Threats in 5G Network. InInternational Conference on Advanced Information Networking and Applications 2023 Mar 15 (pp. 480-489). Cham: Springer International Publishing.

[150] Nguyen VL, Hwang RH, Cheng BC, Lin YD, Duong TQ. Understanding Privacy Risks of High-accuracy Radio Positioning and Sensing in Wireless Networks. IEEE Communications Magazine. 2023 Dec 12.

[151] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[152] Elmaghraby AS, Losavio MM. Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research. 2014 Jul 1, 5(4):491-7.

[153] Zhong M, Yang Y, Yao H, Fu X, Dobre OA, Postolache O. 5G and IoT: Towards a new era of communications and measurements. IEEE Instrumentation & Measurement Magazine. 2019 Nov 28, 22(6):18-26.

[154] Tawalbeh LA, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and security: Challenges and solutions. Applied Sciences. 2020 Jun 15, 10(12):4102.

[155] Ullah A, Azeem M, Ashraf H, Alaboudi AA, Humayun M, Jhanjhi NZ. Secure healthcare data aggregation and transmission in IoT—A survey. IEEE Access. 2021 Jan 19, 9:16849-65.

[156] Diraco G, Rescio G, Caroppo A, Manni A, Leone A. Human action recognition in smart living services and applications: context awareness, data availability, personalization, and privacy. Sensors. 2023 Jun 29, 23(13):6040.

[157] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23, 19(1):e0296781.

[158] Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A. Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine. 2018 Mar, 2(1):36-43.

[159] Patwary MN, Nawaz SJ, Rahman MA, Sharma SK, Rashid MM, Barnes SJ. The potential short-and long-term disruptions and transformative impacts of 5G and beyond wireless networks: Lessons learnt from the development of a 5G testbed environment. Ieee Access. 2020 Jan 7, 8:11352-79.

[160] Kreuter F, Haas GC, Keusch F, Bähr S, Trappmann M. Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. Social Science Computer Review. 2020 Oct, 38(5):533-49.

[161] Taleb T, Mada B, Corici MI, Nakao A, Flinck H. PERMIT: Network slicing for personalized 5G mobile telecommunications. IEEE Communications Magazine. 2017 May 12, 55(5):88-93.

[162] Salahdine F, Liu Q, Han T. Towards secure and intelligent network slicing for 5g networks. IEEE Open Journal of the Computer Society. 2022 Mar 24, 3:23-38.

[163] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[164] Phillips M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). Human genetics. 2018 Aug, 137:575-82.

[165] Wang CX, Di Renzo M, Stanczak S, Wang S, Larsson EG. Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges. IEEE Wireless Communications. 2020 Feb, 27(1):16-23.

[166] Kaur J, Khan MA, Iftikhar M, Imran M, Haq QE. Machine learning techniques for 5G and beyond. IEEE Access. 2021 Jan 13, 9:23472-88.

[167] Rodrigues R. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology. 2020 Dec 1, 4:100005.

[168] Elbamby MS, Perfecto C, Liu CF, Park J, Samarakoon S, Chen X, Bennis M. Wireless edge computing with latency and reliability guarantees. Proceedings of the IEEE. 2019 Jun 11, 107(8):1717-37.

[169] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[170] Varghese B, Villari M, Rana O, James P, Shah T, Fazio M, Ranjan R. Realizing edge marketplaces: Challenges and opportunities. IEEE Cloud Computing. 2018 Nov 29, 5(6):9-20.

[171] Banafaa M, Pepeoğlu Ö, Shayea I, Alhammadi A, Shamsan Z, Razaz MA, Alsagabi M, Al-Sowayan S. A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges. IEEE Access. 2024 Jan 2.

[172] Khan JI. Next-Generation National Communication Infrastructure (NCI): Emerging Future Technologies—Challenges and Opportunities. Functional Reverse Engineering of Machine Tools. 2019 Sep 23:277-307.

[173] Changazi SA, Bakhshi AD, Yousaf M, Mohsin SM, Akber SM, Abazeed M, Ali M. Optimization of network topology robustness in IoTs: A systematic review. Computer Networks. 2024 Jun 6:110568.

[174] Xu Y, Gui G, Gacanin H, Adachi F. A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges. IEEE Communications Surveys & Tutorials. 2021 Feb 17, 23(2):668-95.

[175] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[176] Hu F, Chen B, Zhu K. Full spectrum sharing in cognitive radio networks toward 5G: A survey. IEEE Access. 2018 Feb 5, 6:15754-76.

[177] Catherwood PA, Black B, Mohamed EB, Cheema AA, Rafferty J, McLaughlin JA. Radio channel characterization of mid-band 5G service delivery for ultra-low altitude aerial base stations. IEEE Access. 2019 Jan 10, 7:8283-99.

[178] Malygin KP, Nosov AV. Effect of the Distance Between the Non-Core Turns of a Meander Microstrip Line on the Attenuation of the Interfering Ultrashort Pulse and Signal Integrity. IEEE Electromagnetic Compatibility Magazine. 2023 Dec 18, 12(3):45-54.

[179] Al-Falahy N, Alani OY. Millimetre wave frequency band as a candidate spectrum for 5G network architecture: A survey. Physical Communication. 2019 Feb 1, 32:120-44.

[180] Kaur T, Sharma Y, Sikand R. Futuristic aspects of Li-Fi technology. InAIP Conference Proceedings 2024 Jul 11 (Vol. 3121, No. 1). AIP Publishing.

[181] Zhang H, Ma J, Qiu Z, Yao J, Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Multi-GPU Parallel Pipeline Rendering with Splitting Frame. InComputer Graphics International Conference 2023 Aug 28 (pp. 223-235). Cham: Springer Nature Switzerland.

[182] Haibeh LA, Yagoub MC, Jarray A. A survey on mobile edge computing infrastructure: Design, resource management, and optimization approaches. IEEE Access. 2022 Feb 18, 10:27591-610.

[183] Zanzi L, Sciancalepore V, Garcia-Saavedra A, Schotten HD, Costa-Pérez X. LACO: A latency-driven network slicing orchestration in beyond-5G networks. IEEE Transactions on Wireless Communications. 2020 Oct 7, 20(1):667-82.

[184] Ge X, Yang J, Gharavi H, Sun Y. Energy efficiency challenges of 5G small cell networks. IEEE communications Magazine. 2017 May 12, 55(5):184-91.

[185] Siddiqi MA, Yu H, Joung J. 5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices. Electronics. 2019 Sep 2, 8(9):981.

[186] Suthar P, Agarwal V, Shetty RS, Jangam A. Migration and interworking between 4G and 5G. In2020 IEEE 3rd 5G World Forum (5GWF) 2020 Sep 10 (pp. 401-406). IEEE.

[187] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[188] Banović-Ćurguz N, Ilišević D. Mapping of QoS/QoE in 5G networks. In2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2019 May 20 (pp. 404-408). IEEE.

[189] Martin A, Egaña J, Flórez J, Montalban J, Olaizola IG, Quartulli M, Viola R, Zorrilla M. Network resource allocation system for QoE-aware delivery of media services in 5G networks. IEEE Transactions on Broadcasting. 2018 May 4, 64(2):561-74.

[190] Mattisson S. An overview of 5G requirements and future wireless networks: Accommodating scaling technology. IEEE Solid-State Circuits Magazine. 2018 Aug 26, 10(3):54-60.ax

[191] Zorzi M, Zanella A, Testolin A, De Grazia MD, Zorzi M. Cognition-based networks: A new perspective on network optimization using learning and distributed intelligence. IEEE Access. 2015 Aug 21, 3:1512-30.

[192] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems. 2020 Sep 1, 77:103201.

[193] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[194] Gadallah WG, Ibrahim HM, Omar NM. A deep learning technique to detect distributed denial of service attacks in software-defined networks. Computers & Security. 2024 Feb 1, 137:103588.

[195] Oughton EJ, Frias Z, van der Gaast S, van der Berg R. Assessing the capacity, coverage and cost of 5G infrastructure strategies: Analysis of the Netherlands. Telematics and Informatics. 2019 Apr 1, 37:50-69.

[196] Choi J, Marojevic V, Dietrich CB, Reed JH, Ahn S. Survey of spectrum regulation for intelligent transportation systems. IEEE Access. 2020 Jul 29, 8:140145-60.

[197] Park JH, Rathore S, Singh SK, Salim MM, Azzaoui AE, Kim TW, Pan Y, Park JH. A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. Hum.-Centric Comput. Inf. Sci. 2021 Jan 29, 11(3).

[198] Danjuma UM, Usman KD, Alam AJ, Abdullahi M. Enhancing Security of 5G-Enabled IoT Systems through Advanced Authentication Mechanisms: A Multifaceted Approach. UMYU Scientifica. 2023 Dec 30, 2(4):201-11.

[199] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1, 24:100969.

[200] Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. Digital health. 2023 May, 9:20552076231177144.

[201] Sinigaglia F, Carbone R, Costa G, Zannone N. A survey on multi-factor authentication for online banking in the wild. Computers & Security. 2020 Aug 1, 95:101745.

[202] Cárdenas A, Fernández D, Lentisco CM, Moyano RF, Bellido L. Enhancing a 5G network slicing management model to improve the support of mobile virtual network operators. IEEE Access. 2021 Sep 22, 9:131382-99.

[203] Ilori O, Nwosu NT, Naiho HN. Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies.

[204] Itani D, Itani R, Eltweri AA, Faccia A, Wanganoo L. Enhancing Cybersecurity Through Compliance and Auditing: A Strategic Approach to Resilience. In2024 2nd International Conference on Cyber Resilience (ICCR) 2024 Feb 26 (pp. 1-10). IEEE.

[205] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[206] Huso I, Olivieri M, Galgano L, Rashid A, Piro G, Boggia G. Design and implementation of a looking-forward Lawful Interception architecture for future mobile communication systems. Computer Networks. 2024 Jul 1, 249:110518.

[207] Vaishnavi A, Pillai S. Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. InJournal of Physics: Conference Series 2021 Jul 1 (Vol. 1964, No. 4, p. 042002). IOP Publishing.

[208] Cheng JK, Lim EM, Krikorian YY, Sklar DJ, Kong VJ. A survey of encryption standard and potential impact due to quantum computing. In2021 IEEE Aerospace Conference (50100) 2021 Mar 6 (pp. 1-10). IEEE.

[209] Njorbuenwu M, Swar B, Zavarsky P. A survey on the impacts of quantum computers on information security. In2019 2nd International conference on data intelligence and security (ICDIS) 2019 Jun 28 (pp. 212-218). IEEE.

[210] Kebande VR, Awaysheh FM, Ikuesan RA, Alawadi SA, Alshehri MD. A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. Sensors. 2021 Sep 8, 21(18):6018.

[211] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[212] Tyler D, Viana T. Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences. 2021 Aug 16, 11(16):7499.

[213] Venkatraman S, Parvin S. Developing an IoT identity management system using blockchain. Systems. 2022 Apr, 10(2):39.

[214] Afolabi I, Taleb T, Samdanis K, Ksentini A, Flinck H. Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. IEEE Communications Surveys & Tutorials. 2018 Mar 21, 20(3):2429-53.

[215] Al-Muhtadi J, Saleem K, Al-Rabiaah S, Imran M, Gawanmeh A, Rodrigues JJ. A lightweight cyber security framework with context-awareness for pervasive computing environments. Sustainable Cities and Society. 2021 Mar 1, 66:102610.

[216] Maleh Y, Qasmaoui Y, El Gholami K, Sadqi Y, Mounir S. A comprehensive survey on SDN security: threats, mitigations, and future directions. Journal of Reliable Intelligent Environments. 2023 Jun, 9(2):201-39.

[217] Mazher AN, Waleed J, MaoLood AT. The Security Threats and Solutions of Network Functions Virtualization: A Review. Journal of Al-Qadisiyah for computer science and mathematics. 2020 Dec 25, 12(4):Page-38.

[218] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[219] Lu G, Koufteros X, Lucianetti L. Supply chain security: A classification of practices and an empirical study of differential effects and complementarity. IEEE Transactions on Engineering Management. 2017 Feb 2, 64(2):234-48.

[220] Gudala L, Shaik M, Venkataramanan S, Sadhu AK. Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks. Distributed Learning and Broad Applications in Scientific Research. 2019 Jul 5, 5:23-54.

[221] Gudala L, Shaik M, Venkataramanan S. Leveraging Machine Learning for Enhanced Threat Detection and Response in Zero Trust Security Frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. Journal of Artificial Intelligence Research. 2021 Nov 26, 1(2):19-45.

[222] Hays S, White DJ. Employing llms for incident response planning and review. arXiv preprint arXiv:2403.01271. 2024 Mar 2.

[223] Tatineni S. Cloud-Based Business Continuity and Disaster Recovery Strategies. International Research Journal of Modernization in Engineering, Technology, and Science. 2023 Nov, 5(11):1389-97.

[224] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[225] Saqib N, Germanos V, Zeng W, Maglaras L. Mapping of the Security Requirements of GDPR and NISD. EAI Endorsed Transactions on Security and Safety. 2020 Sep 3, 7(24).

[226] Pelluru K. Integrate security practices and compliance requirements into DevOps processes. MZ Computing Journal. 2021 Sep 16, 2(2):1-9.

[227] Dutta A, Hammad E. 5G security challenges and opportunities: A system approach. In2020 IEEE 3rd 5G world forum (5GWF) 2020 Sep 10 (pp. 109-114). IEEE.

[228] Rajapakse RN, Zahedi M, Babar MA, Shen H. Challenges and solutions when adopting DevSecOps: A systematic review. Information and software technology. 2022 Jan 1, 141:106700.

[229] Sharma R, Arya R. Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Transactions on Emerging Telecommunications Technologies. 2023 Nov, 34(11):e4571.

[230] James E, Rabbi F. Fortifying the IoT landscape: Strategies to counter security risks in connected systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries. 2023 Jan 9, 6(1):32-46.

[231] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31, 47(6).

[232] Rezaee K, Rezakhani SM, Khosravi MR, Moghimi MK. A survey on deep learning-based real-time crowd anomaly detection for secure distributed video surveillance. Personal and Ubiquitous Computing. 2024 Feb, 28(1):135-51.

[233] Zawoad S, Dutta AK, Hasan R. Towards building forensics enabled cloud through secure logging-as-a-service. IEEE Transactions on Dependable and Secure Computing. 2015 Sep 25, 13(2):148-62.

[234] Farhood ZK, Abed AA, Al-Shareeda S. SHADOW: Silent-based Hybrid Approach for Dynamic Pseudonymization and Privacy Preservation in Vehicular Networks. InAsia Simulation Conference 2023 Oct 13 (pp. 421-440). Singapore: Springer Nature Singapore.

[235] Liu L, Li J, Lv J, Wang J, Zhao S, Lu Q. Privacy-Preserving and Secure Industrial Big Data Analytics: A Survey and the Research Framework. IEEE Internet of Things Journal. 2024 Jan 15.

[236] Kishor K. Personalized federated learning. InFederated Learning for IoT Applications 2022 Feb 2 (pp. 31-52). Cham: Springer International Publishing.

[237] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9, 3(5):364.

[238] Vithalkar PN. Cryptographic Protocols Resilient to Quantum Attacks: Advancements in Post-Quantum Cryptography. Communications on Applied Nonlinear Analysis. 2024 Jun 23, 31(3s):520-32.

[239] Shaw G, Isika Ghosh KK, Bose H, Singh J, Majumdar A, Ghosal A, Biswas S. The Evolution of IoT Applications in Smart Homes and Smart Cities: A 2019-2024 Analysis.

[240] Prybylo M, Haghighi S, Peddinti ST, Ghanavati S. Evaluating Privacy Perceptions, Experience, and Behavior of Software Development Teams. arXiv preprint arXiv:2404.01283. 2024 Apr 1.

[241] Akhtar N, Kerim B, Perwej Y, Tiwari A, Praveen S. A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science Engineering and Technology. 2021 Sep 18.

[242] Nandakumar K, Vinod V, Akbar Batcha SM, Sharma DK, Elangovan M, Poonia A, Mudlappa Basavaraju S, Dogiwal SR, Dadheech P, Sengan S. Securing data in transit using data-in-transit defender architecture for cloud communication. Soft Computing. 2021 Sep, 25(18):12343-56.

[243] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[244] Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: A review. IEEE Access. 2021 Jan 21, 9:18706-21.

[245] Khaleel TA. Developing robust machine learning models to defend against adversarial attacks in the field of cybersecurity. In2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2024 May 23 (pp. 1-7). IEEE.

[246] Seeman J, Susser D. Between privacy and utility: On differential privacy in theory and practice. ACM Journal on Responsible Computing. 2024 Mar 20, 1(1):1-8.

[247] Su G, Wang J, Xu X, Wang Y, Wang C. The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology. 2024 Mar 13, 2(1):52-8.

[248] Carlson G, McKinney J, Slezak E, Wilmot ES. General Data Protection Regulation and California Consumer Privacy Act: Background. Currents: J. Int'l Econ. L.. 2020, 24:62.

[249] Bozkus Kahyaoglu S, Caliyurt K. Cyber security assurance process from the internal audit perspective. Managerial auditing journal. 2018 Jun 6, 33(4):360-76.

[250] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[251] Liyanage M, Salo J, Braeken A, Kumar T, Seneviratne S, Ylianttila M. 5G privacy: Scenarios and solutions. In2018 IEEE 5G World Forum (5GWF) 2018 Jul 9 (pp. 197-203). IEEE.

[252] Becher S, Gerl A, Meier B, Bölz F. Big picture on privacy enhancing technologies in e-health: a holistic personal privacy workflow. Information. 2020 Jul 8, 11(7):356.

[253] Maddireddy BR, Maddireddy BR. Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management. Unique Endeavor in Business & Social Sciences. 2022 Jun 30, 1(2):47-62.

[254] He S, Zhu J, He P, Lyu MR. Experience report: System log analysis for anomaly detection. In2016 IEEE 27th international symposium on software reliability engineering (ISSRE) 2016 Oct 23 (pp. 207-218). IEEE.

[255] Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine. 2023 May 1, 158:106848.

[256] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[257] Liu H, Crespo RG, Martínez OS. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. InHealthcare 2020 Jul 29 (Vol. 8, No. 3, p. 243). MDPI.

[258] Banditwattanawong T, Masdisornchote M, Uthayopas P. Multi-provider cloud computing network infrastructure optimization. Future Generation Computer Systems. 2016 Feb 1, 55:116-28.

[259] Perera L, Ranaweera P, Kusaladharma S, Wang S, Liyanage M. Unlocking Spectrum Potential: A Blockchain-Powered Paradigm for Dynamic Spectrum Management. In2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) 2024 Jun 3 (pp. 1181-1186). IEEE.

[260] Hodaei A, Babaie S. A survey on traffic management in software-defined networks: challenges, effective approaches, and potential measures. Wireless Personal Communications. 2021 May, 118(2):1507-34.

[261] Bordel B, Alcarria R, Robles T, Sanchez-de-Rivera D. Service management in virtualization-based architectures for 5G systems with network slicing. Integrated Computer-Aided Engineering. 2020 Jan 1, 27(1):77-99.

[262] Ramzan MR, Nawaz N, Ahmed A, Naeem M, Iqbal M, Anpalagan A. Multi-objective optimization for spectrum sharing in cognitive radio networks: A review. Pervasive and Mobile Computing. 2017 Oct 1, 41:106-31.

[263] Frieden R. The evolving 5G case study in spectrum management and industrial policy. Telecommunications Policy. 2019 Jul 1, 43(6):549-62.

[264] Borralho R, Mohamed A, Quddus AU, Vieira P, Tafazolli R. A survey on coverage enhancement in cellular networks: Challenges and solutions for future deployments. IEEE Communications Surveys & Tutorials. 2021 Jan 21, 23(2):1302-41.

[265] Zhang Z. Massive MIMO technology: a key advancement in shaping communication networks for the 5G/5G+ era. In2024 International Wireless Communications and Mobile Computing (IWCMC) 2024 May 27 (pp. 274-278). IEEE.

[266] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[267] Mollahasani S, Eroğlu A, Demirkol I, Onur E. Density-aware mobile networks: Opportunities and challenges. Computer networks. 2020 Jul 5, 175:107271.

[268] Zhang H, Chu X, Guo W, Wang S. Coexistence of Wi-Fi and heterogeneous small cell networks sharing unlicensed spectrum. IEEE communications magazine. 2015 Mar 18, 53(3):158-64.

[269] Sharma T, Chehri A, Fortier P. Review of optical and wireless backhaul networks and emerging trends of next generation 5G and 6G technologies. Transactions on Emerging Telecommunications Technologies. 2021 Mar, 32(3):e4155.

[270] Sousa I, Sousa N, Queluz MP, Rodrigues A. Fronthaul design for wireless networks. Applied Sciences. 2020 Jul 10, 10(14):4754.

[271] Spinelli F, Mancuso V. Toward enabled industrial verticals in 5G: A survey on MEC-based approaches to provisioning and flexibility. IEEE Communications Surveys & Tutorials. 2020 Nov 12, 23(1):596-630.

[272] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[273] Bilal K, Khalid O, Erbad A, Khan SU. Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers. Computer Networks. 2018 Jan 15, 130:94-120.

[274] Marinova S, Lin T, Bannazadeh H, Leon-Garcia A. End-to-end network slicing for future wireless in multi-region cloud platforms. Computer Networks. 2020 Aug 4, 177:107298.

[275] Afolabi I, Prados-Garzon J, Bagaa M, Taleb T, Ameigeiras P. Dynamic resource provisioning of a scalable E2E network slicing orchestration system. IEEE Transactions on Mobile Computing. 2019 Jul 25, 19(11):2594-608.

[276] Goswami MJ. Leveraging AI for Cost Efficiency and Optimized Cloud Resource Management. International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal. 2020, 7(1):21-7.

[277] Fu Y, Wang S, Wang CX, Hong X, McLaughlin S. Artificial intelligence to manage network traffic of 5G wireless networks. IEEE network. 2018 Nov 29, 32(6):58-64.

[278] Beshley M, Kryvinska N, Seliuchenko M, Beshley H, Shakshuki EM, Yasar AU. End-to-End QoS "smart queue" management algorithms and traffic prioritization mechanisms for narrow-band internet of things services in 4G/5G networks. Sensors. 2020 Apr 19, 20(8):2324.

[279] Narmanlioglu O, Zeydan E, Arslan SS. Service-aware multi-resource allocation in software-defined next generation cellular networks. Ieee Access. 2018 Mar 23, 6:20348-63.

[280] Keshkar M, Muthalagu R, Rajak A, Mathew LK. GAE and OBE enhanced interference mitigation techniques in LDACS. Aerospace. 2022 Jan 17, 9(1):45.

[281] Ahmad WS, Radzi NA, Samidi FS, Ismail A, Abdullah F, Jamaludin MZ, Zakaria M. 5G technology: Towards dynamic spectrum sharing using cognitive radio networks. IEEE access. 2020 Jan 13, 8:14460-88.

[282] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[283] von Tüllenburg F, Dorfinger P, Veichtlbauer A, Pache U, Langthaler O, Kapoun H, Bischof C, Kupzog F. Virtualising redundancy of power equipment controllers using software-defined networking. Energy Informatics. 2019 Sep, 2:1-20.

[284] Wang J, Jin A, Shi D, Wang L, Shen H, Wu D, Hu L, Gu L, Lu L, Chen Y, Wang J. Spectral efficiency improvement with 5G technologies: Results from field tests. IEEE Journal on Selected Areas in Communications. 2017 Jun 8, 35(8):1867-75.

[285] Gures E, Shayea I, Alhammadi A, Ergen M, Mohamad H. A comprehensive survey on mobility management in 5G heterogeneous networks: Architectures, challenges and solutions. IEEE Access. 2020 Oct 13, 8:195883-913.

[286] Saleem D, Sundararajan A, Sanghvi A, Rivera J, Sarwat AI, Kroposki B. A multidimensional holistic framework for the security of distributed energy and control systems. IEEE Systems Journal. 2019 Jul 3, 14(1):17-27.

[287] Varanda A, Santos L, Costa RL, Oliveira A, Rabadão C. Log pseudonymization: Privacy maintenance in practice. Journal of Information Security and Applications. 2021 Dec 1, 63:103021.

[288] Paya A, Gómez A. Securesdp: a novel software-defined perimeter implementation for enhanced network security and scalability. International Journal of Information Security. 2024 May 20:1-6.

[289] Saad SA, Shayea I, Ahmed NM. Artificial intelligence linear regression model for mobility robustness optimization algorithm in 5G cellular networks. Alexandria Engineering Journal. 2024 Feb 1, 89:125-48.

[290] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28, 15(13):10264.

[291] Zhang Y, Sun R, Shen L, Bai G, Xue M, Meng MH, Li X, Ko R, Nepal S. Privacy-preserving and fairness-aware federated learning for critical infrastructure protection and resilience. InProceedings of the ACM on Web Conference 2024 2024 May 13 (pp. 2986-2997).

[292] Labu MR, Ahammed MF. Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. Journal of Computer Science and Technology Studies. 2024 Feb 13, 6(1):179-88.

[293] Strand M. A status update on quantum safe cryptography. In2021 International conference on military communication and information systems (ICMCIS) 2021 May 4 (pp. 1-7). IEEE.

[294] Pillai SE, Polimetla K. Privacy-Preserving Network Traffic Analysis Using Homomorphic Encryption. In2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) 2024 Feb 23 (pp. 1-6). IEEE.

[295] Chukwurah EG. Leading SAAS innovation within us regulatory boundaries: the role of tpms in navigating compliance. Engineering Science & Technology Journal. 2024 Apr 17, 5(4):1372-85.

[296] Ganesan T, Al-Fatlawy RR, Srinath S, Aluvala S, Kumar RL. Dynamic Resource Allocation-Enabled Distributed Learning as a Service for Vehicular Networks. In2024 Second International Conference on Data Science and Information System (ICDSIS) 2024 May 17 (pp. 1-4). IEEE.

[297] Goumopoulos C, Mavrommati I. A framework for pervasive computing applications based on smart objects and end user development. Journal of Systems and Software. 2020 Apr 1, 162:110496.