






## Article

# A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions

Hussam N. Fakhouri <sup>1</sup>, Sadi Alawadi <sup>2,\*</sup>, Feras M. Awaysheh <sup>3</sup>, Imad Bani Hani <sup>4</sup>,  
Mohannad Alkhalailah <sup>5</sup> and Faten Hamad <sup>6,7</sup>

<sup>1</sup> Data Science and Artificial Intelligence Department, Faculty of Information Technology, University of Petra, Amman 11196, Jordan; hussam.fakhouri@uop.edu.jo

<sup>2</sup> Department of Computer Science (DIDA), Blekinge Institute of Technology, 371 79 Karlskrona, Sweden

<sup>3</sup> Institute of Computer Science, Delta Center, Tartu University, 51009 Tartu, Estonia; feras.awaysheh@ut.ee

<sup>4</sup> Department of Computer Science, Halmstad University, 301 18 Halmstad, Sweden; imad.banihani@hh.se

<sup>5</sup> College of Education, Humanities and Social Sciences, Al Ain University, Al-Ain P.O. Box 112612, United Arab Emirates; mohannad.alkhalailah@aau.ac.ae

<sup>6</sup> Information Studies Department, Sultan Qaboos University, Muscat 123, Oman; f.hamad@ju.edu.jo

<sup>7</sup> Library and Information Science, The University of Jordan, Amman 11180, Jordan

\* Correspondence: sadi.alawadi@bth.se

**Abstract:** Fifth-generation (5G) mobile networks have already marked their presence globally, revolutionizing entertainment, business, healthcare, and other domains. While this leap forward brings numerous advantages in speed and connectivity, it also poses new challenges for security protocols. Machine learning (ML) and deep learning (DL) have been employed to augment traditional security measures, promising to mitigate risks and vulnerabilities. This paper conducts an exhaustive study to assess ML and DL algorithms' role and effectiveness within the 5G security landscape. Also, it offers a profound dissection of the 5G network's security paradigm, particularly emphasizing the transformative role of ML and DL as enabling security tools. This study starts by examining the unique architecture of 5G and its inherent vulnerabilities, contrasting them with emerging threat vectors. Next, we conduct a detailed analysis of the network's underlying segments, such as network slicing, Massive Machine-Type Communications (mMTC), and edge computing, revealing their associated security challenges. By scrutinizing current security protocols and international regulatory impositions, this paper delineates the existing 5G security landscape. Finally, we outline the capabilities of ML and DL in redefining 5G security. We detail their application in enhancing anomaly detection, fortifying predictive security measures, and strengthening intrusion prevention strategies. This research sheds light on the present-day 5G security challenges and offers a visionary perspective, highlighting the intersection of advanced computational methods and future 5G security.

**Keywords:** 5G networks; machine learning security; security in deep learning



**Citation:** Fakhouri, H.N.; Alawadi, S.; Awaysheh, F.M.; Hani, I.B.; Alkhalailah, M.; Hamad, F. A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. *Electronics* **2023**, *12*, 4604. <https://doi.org/10.3390/electronics12224604>

Academic Editor: Heung-Il Suk

Received: 7 September 2023

Revised: 22 October 2023

Accepted: 27 October 2023

Published: 10 November 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The emergence of the fifth-generation (5G) mobile network represents a significant milestone in the field of telecommunications. This advanced technology promises to revolutionize connectivity, ushering in a new era with the potential for transformative impacts on various sectors [1]. As 5G networks provide ultra-high-speed data transmission, minimal latency, and high-density connectivity, they are poised to underpin crucial developments in the Internet of Things (IoT), autonomous vehicles, smart cities, and other technological advancements [2]. As 5G networks increasingly underpin essential sectors such as healthcare, transportation, defense, and public services, robust security measures become paramount to sustain trust, safeguard privacy, and ensure the functional integrity of these sectors [3]. With 5G infrastructure becoming a cornerstone of our digitally oriented society, the intricate and pervasive nature of its security implications necessitates thorough scholarly exploration.

Recent research has highlighted the centrality of 5G security in sustaining the reliability and integrity of 5G services [4]. The susceptibility of 5G networks to cyberattacks, both from known and unidentified sources, has been a focal concern [5]. The necessity for dynamic and adaptive security solutions has been pointed out by several scholars, emphasizing the need for innovative approaches to combat evolving cyber threats [6]. While conventional methods of cybersecurity have been effective to a degree, the exponential increase in data volumes, device heterogeneity, and system complexity inherent in 5G networks necessitate the exploration of more innovative, dynamic, and adaptive security measures. To this end, artificial intelligence (AI) branches such as machine learning (ML) and deep learning (DL) have been increasingly recognized as pivotal in strengthening 5G security [7]. Leveraging the power of these AI subdomains is critical in examining their promising roles in fortifying 5G networks against a myriad of potential cyber threats.

ML, with its ability to learn and improve from experience, provides a robust framework for identifying patterns, detecting anomalies, and predicting potential threats, thereby enhancing the effectiveness and efficiency of security solutions [8]. On the other hand, DL, a subset of ML that imitates the functioning of the human brain in processing data, offers a deeper layer of security by recognizing and mitigating complex cyberattacks in real time [9]. The pivot to 5G is not just a technological shift; it is an evolutionary leap that brings unique challenges, many of which remain uncharted in current research, like big data [10]. Using ML and DL, the promise these techniques hold for security is yet to be fully harnessed, especially tailored for 5G's dynamic environment. Given our escalating dependence on 5G infrastructures and the palpable risks of security oversights, there is a pressing imperative to delve deeper, to preemptively identify vulnerabilities, and to devise robust countermeasures.

This research delves into these areas, shedding light on how ML and DL can be leveraged to ensure 5G security. Also, it seeks to fill this void by providing a comprehensive examination of 5G security, tracing its evolution, dissecting the associated threats, and probing the effectiveness of current and prospective security solutions. Furthermore, it explores the role of ML and DL in various areas of 5G security, including intrusion detection, risk prediction, security protocol optimization, and more. It also aims to provide a holistic perspective on the potential of ML and DL in enhancing 5G security. It also intends to address the challenges and limitations encountered in integrating these advanced technologies into 5G networks and offers potential solutions in this exciting area of research. This research, therefore, embarks on an exhaustive exploration into the world of 5G security, with a keen focus on the revolutionary potential of ML and DL. In doing so, we aim to offer a comprehensive resource that not only illuminates the current challenges but also paves the way for future innovations in the realm of 5G security.

### *1.1. Study Objectives*

This study aims to thoroughly examine security concerns and strategies within 5G mobile technology while also investigating ML and DL's roles in addressing these security issues. Thus, this study seeks to identify the distinctive security challenges inherent to the 5G system, comprehend their broader implications, and critically assess the efficacy of potential solutions. Further, this research provides a broad overview of 5G telecommunications technology, highlighting its technical aspects, architecture, and technical aspects. Secondly, this study examines the primacy of security in 5G networks and discusses the privacy concerns and the importance of ensuring the reliability and integrity of services. Thirdly, this research explores the role of ML and DL in enhancing 5G mobile technology security. Also, this research aims to dissect the theoretical underpinnings of existing security mechanisms using AI, shedding light on the concepts and principles that undergird the current security landscape of 5G networks.

This research aims to answer the following key questions:

1. What are the unique security challenges posed by 5G telecommunications technology?
2. What are the solutions for the security challenges of 5G telecommunications technology?

3. What is the role of machine learning and deep learning in enhancing 5G mobile technology security?

### *1.2. Study Contributions*

In this research, we present an exhaustive examination of security dimensions in 5G networks. The contributions emanating from this scholarly endeavor encompass the following: (1) An extensive exposition of the current security architectures and functionalities deployed in 5G networks. (2) An in-depth analysis of security threats and security breaches in 5G networks. (3) Another salient contribution is an in-depth exploration of the unique security challenges arising from 5G's features. These challenges effectively expand the existing threat landscape of 5G networks. (4) An analysis of the security issues in Massive Machine-Type Communications (mMTC), network slicing vulnerabilities, and their associated mitigation strategies in 5G networks. (5) An in-depth analysis of the role of machine learning and deep learning techniques in enhancing 5G security.

### *1.3. Methodology*

This study adopts a systematic literature review methodology to investigate security concerns in 5G networks. The search strategy encompasses several academic databases, such as IEEE Xplore, ACM Digital Library, and Google Scholar, focusing on recent peer-reviewed articles and conference proceedings. Specific keywords, such as "5G Security", "5G vulnerabilities", "Machine learning in 5G security", and "Network attacks in 5G", were employed to narrow the scope of the inquiry. Upon identifying potential articles, an initial screening process was conducted based on titles and abstracts to assess relevance. The selected articles then underwent a more rigorous full-text evaluation to ascertain their alignment with the research objectives. Quality metrics include the reputation of the publication outlet, the rigor of the methodologies employed, and citation frequency, among others. Data extracted from each vetted article include research objectives, methods, key findings, and implications. Thematic analysis was subsequently employed to identify and interpret patterns related to 5G security and machine learning and deep learning in enhancing 5G security, answering this study's research questions. This approach ensures that the findings are rigorous and pertinent to the domain of 5G security.

The rest of the paper is organized as follows. Section 2 discusses 5G telecommunications technology and architecture. Section 3 examines in detail the mobile network security evolution and the evolution of the threat landscape. Section 4 explores and analyzes the security threat landscape in 5G networks. Section 5 discusses the current and prospective solutions to enhance 5G security. Sections 6 and 7 discuss the role of machine learning and deep learning in 5G security and the cutting-edge technologies being applied or proposed to address 5G security concerns. Section 8 discusses the technical and ethical considerations for the effective implementation of 5G security. Finally, Section 9 draws this study's conclusions and guidelines for future work.

## **2. Fifth-Generation Telecommunications Technology and Architecture**

In order to better understand the security threats and challenges that face 5G technology, we will start by analyzing the 5G network technology and architecture in detail; 5G, the fifth generation of mobile networks, represents a substantial technological leap in telecommunications technology, laying the foundation for a hyper-connected world. Marking a significant departure from its predecessors, 5G's infrastructure has been designed to enable an array of new services, cater to increasingly dense traffic, support massive device connectivity, and offer high-speed data transfer with ultra-low latency. At the core of 5G technology are a set of new technologies and concepts, including advanced antenna techniques, beamforming, massive Multiple-Input Multiple-Output (MIMO), Network Function Virtualization (NFV), Software-Defined Networking (SDN), and Mobile Edge Computing (MEC), among others [11]. Together, these technologies enable 5G networks to offer unprecedented network performance in terms of speed, capacity, and flexibility.

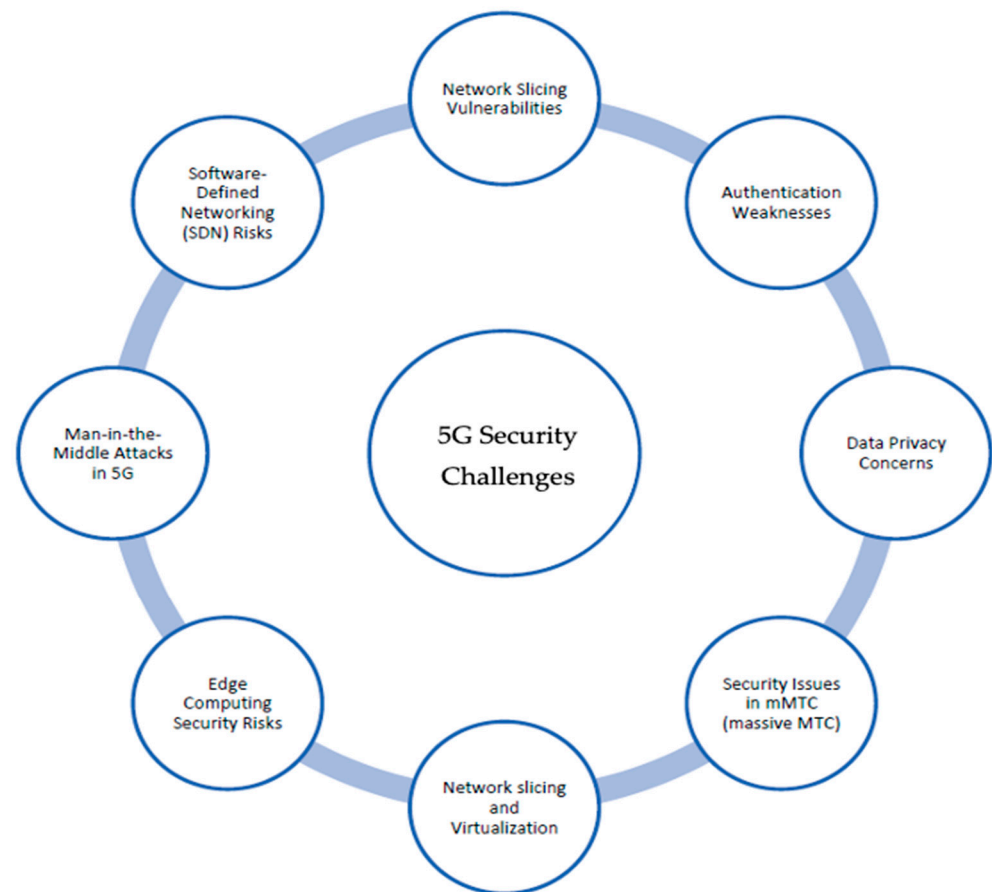
A key differentiating feature of 5G technology is its flexible architecture, allowing it to serve a broad spectrum of use cases, each with its specific requirements. Unlike the previous generations of mobile networks that were primarily designed for human-oriented communication, 5G is intended to support diverse application scenarios encompassing human-oriented and machine-oriented communications [12].

Furthermore, 5G is not simply an evolution of 4G LTE; it brings forth entirely new network paradigms such as dense networking and network slicing, making it possible to customize different network slices for specific use cases or services [13]. This degree of customization is a step towards providing a more personalized, efficient, and secure network experience. One of the most intriguing features of 5G is its spectrum flexibility. While previous mobile network generations primarily operated on sub-6 GHz bands, 5G extends the usable spectrum to higher frequency bands, including millimeter wave bands (up to 100 GHz). The use of these high-frequency bands opens up large amounts of spectrum, enabling higher data rates, reduced latency, and increased capacity [14]. Additionally, 5G networks utilize advanced modulation and coding schemes, as well as sophisticated multi-antenna techniques, to further enhance the data rate and network capacity. These enhancements not only improve the quality of service but also increase the spectral efficiency, ensuring that the network resources are used optimally [15]. While the technical intricacies of 5G networks are complex, the fundamental objective is to build a flexible, efficient, and secure network that can accommodate the increasing demand for connectivity in the modern digital age. An evolution of mobile network security concerns and technology for each generation from 1G to 6G is shown in Table 1.

**Table 1.** Evolution of mobile network security concerns and key technological for each generation [16,17].

Generation	Security Concerns and Measures	Impact on Security	Key Technological Advances
1G	Limited security priorities; primarily focused on basic voice communication.	Minimal impact; minimal data vulnerabilities	- Analog voice calls
2G	Digital data vulnerability; introduced encryption methods like A5/1	Increased security with encryption; vulnerabilities like A5/1 attacks	- Digital communication - A5/1 encryption
3G	Broadened threat landscape; robust encryption and authentication required	Improved security with robust encryption; counteracted malware and phishing	- IP-based services - Robust encryption - User-network authentication
4G	Increased vulnerabilities; advanced security measures adopted	Enhanced security with advanced encryption; focus on all-IP networks	- Advanced encryption - Secure IP-based protocols - All-IP architecture
5G	New security challenges; dynamic security solutions needed; ML and DL adoption	Heightened security challenges; dynamic security solutions; ML and DL usage	- Network slicing - MIMO - Network Function Virtualization - Software-Defined Networking - Mobile edge computing - Flexible architecture - Spectrum flexibility
6G	Potential security challenges; reliance on AI; terahertz frequencies	Expected security enhancements with AI; potential risks with AI manipulation	- Terahertz frequencies - Cell-free architectures - Satellite-network integration - Quantum encryption - Collaborative AI-driven defenses

Table 1 seeks to delineate this evolution by mapping each generation of mobile networks to its associated security concerns, the impact these concerns have on security, and the key technological advances introduced in each era. As the table elucidates, security measures have evolved from minimal concerns in 1G, primarily focused on voice communications, to multifaceted strategies in 5G that leverage ML and DL techniques for dynamic security solutions. The anticipated 6G technology is poised to bring its own set of challenges and solutions, potentially hinging on artificial intelligence (AI) and quantum encryption. The 5G security challenges are shown in Figure 1:



**Figure 1.** Fifth-generation security challenges.

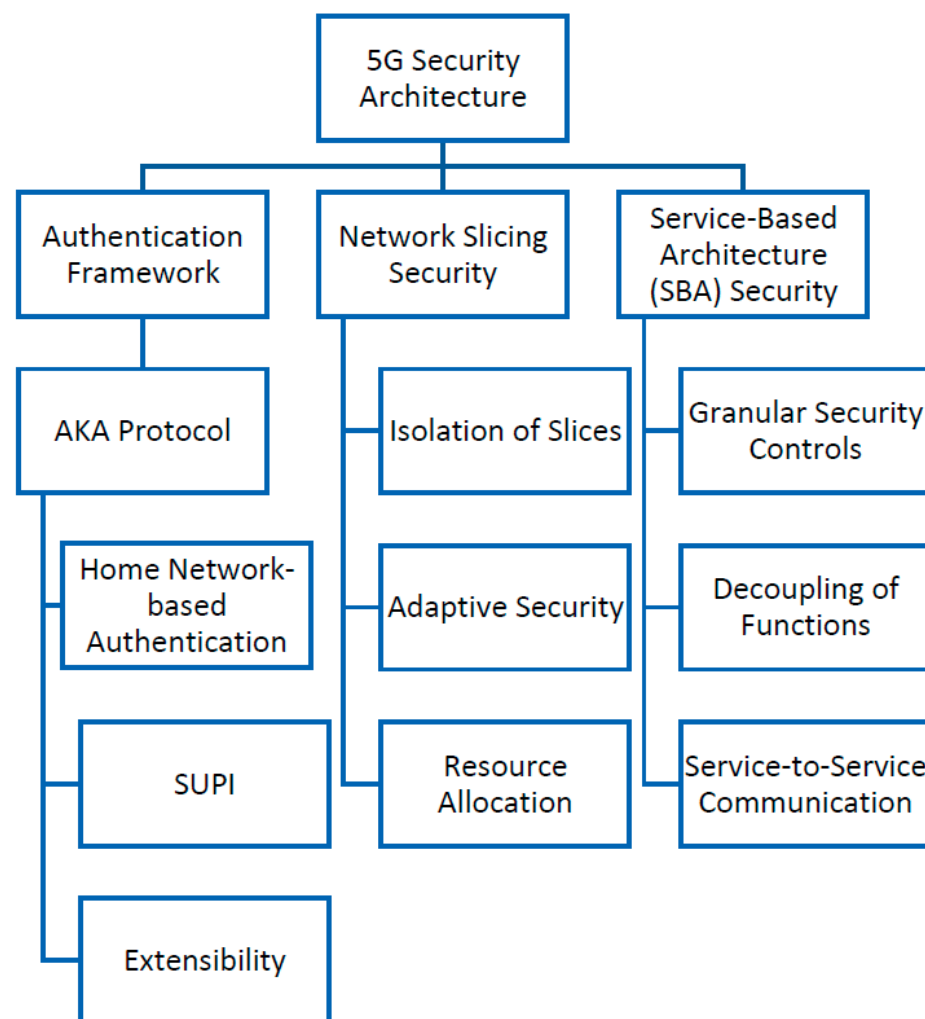
### 2.1. Network Architecture in 5G

The 5G network architecture is a radical departure from the previous generations, insofar as it is characterized by increased flexibility and adaptability. Unlike the preceding generations of mobile networks, which were primarily built around a rigid, hierarchical network structure, the 5G architecture is designed to be highly flexible, distributed, and software-defined. It incorporates a wide range of innovative concepts and techniques, such as network slicing, edge computing, and SDN, which collectively contribute to enhanced performance, functionality, and user experience [18].

The design of 5G network architecture addresses several requirements and challenges brought about by a range of applications, from high-speed mobile broadband to ultra-reliable, low-latency communications (uRLLC) [19]. The versatility and adaptability of 5G structures stem from a transition to a more software-centric approach from a traditionally hardware-centric one, enabling a level of flexibility, scalability, and efficiency never seen before in previous generations. Fifth-generation networks employ a heterogeneous network (HetNet) structure that supports the coexistence of different types of cells, varying from macro-cells to small cells like pico-cells and femtocells. The utilization of these different cell types in a layered structure optimizes coverage and capacity, especially in dense urban



environments, and ensures a more uniform user experience [20]. The core characteristic of 5G network structure is its use of a flat, decentralized architecture instead of the traditional hierarchical one, to reduce latency and optimize traffic routing. The use of decentralized architectures also allows for higher throughput rates, enabling faster data transmission [21]. To deal with the demand for high data rates and the massive connectivity required for IoT devices, 5G also includes the use of advanced antenna technologies, such as MIMO. Massive MIMO increases the capacity of a cell by using a high number of transmit antennas at the base station to serve a significant number of users in the same time–frequency resource [22]. Crucially, 5G networks implement a cloud-based architecture where functions and services can be instantiated in a flexible and dynamic manner [23]. This leads to a paradigm shift from a dedicated hardware-centric infrastructure to a more flexible, software-centric environment, enhancing the adaptability and scalability of network services. A diagrammatical illustration of 5G network architecture is shown in Figure 2.



**Figure 2.** Fifth-generation security architecture.

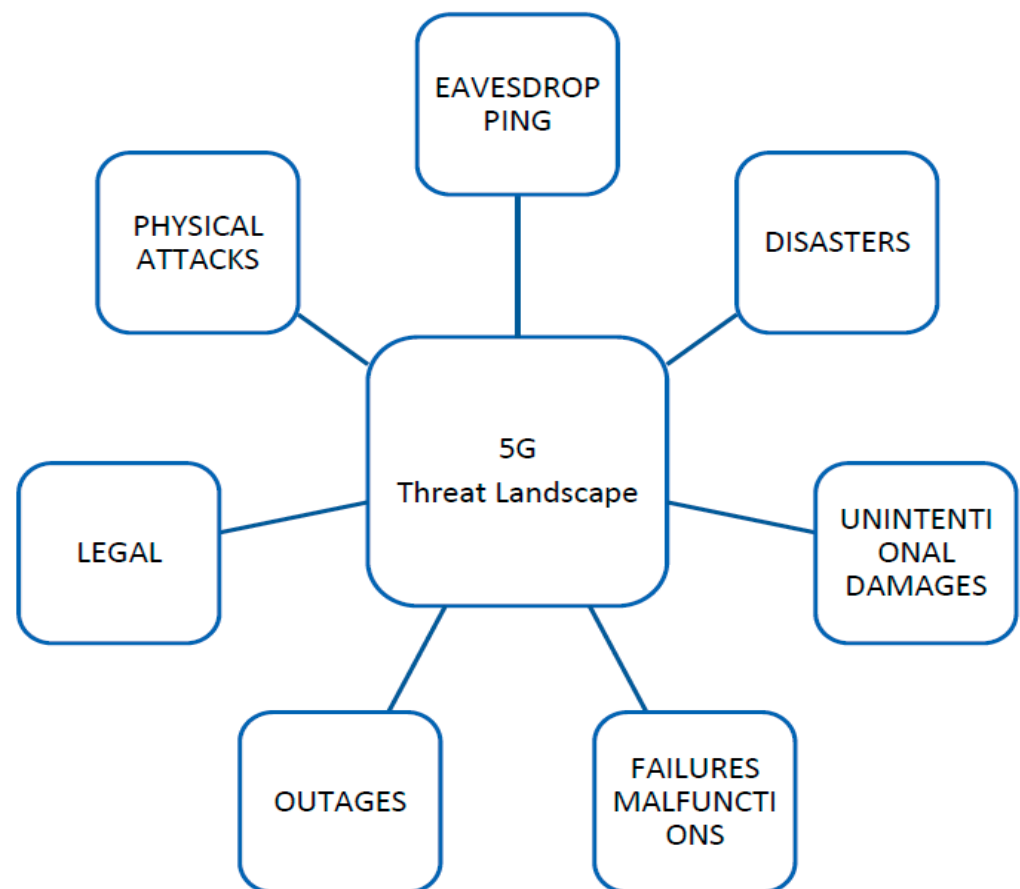
#### Key Elements of 5G Architecture

The architecture of 5G networks is an amalgamation of various key components, each playing a vital role in providing superior performance, high-speed connectivity, and greater adaptability (see Figure 3). In this section, we explore these integral elements, offering an in-depth understanding of their functionalities:

1. The user equipment (UE): The UE is the endpoint of the communication within the network. This could range from a smartphone or tablet to a connected vehicle or an IoT device. It serves as the primary interface for users to interact with the network [24].

- The UE is designed to support a broad spectrum of frequency bands, enabling it to connect with different types of cells in a heterogeneous network.
2. The 5G new radio (NR) access network: This aspect of the 5G network architecture primarily comprises gNodeBs (next-generation NodeBs), which provide the wireless connectivity between the UE and the core network. They are designed to support massive MIMO and beamforming technologies, which considerably enhance the capacity, coverage, and user experience [25].
  3. The 5G core network: The core network in 5G systems operates as the orchestrator of various network functions and services. Unlike the core networks of previous generations, the 5G core network is characterized by increased virtualization and flexibility. It is built around an SBA, which allows for dynamic and flexible service provisioning. It is responsible for critical tasks like authentication, mobility management, session management, and interconnection with other networks [26].
  4. The network slices: Network slicing is a revolutionary element in 5G architecture. It essentially refers to a logically isolated end-to-end network that can be customized to cater to the specific requirements of a particular service or application. Network slices can be designed with a specific set of optimized resources and network topology that cater to different use case requirements, such as latency, throughput, reliability, and capacity. This separation of resources enables the operator to deploy a multitude of slices, each catering to a specific use case, all the while ensuring that a failure in one does not impact the others [27].
  5. Edge computing: Another vital component of 5G architecture is edge computing, which pushes computational capabilities closer to the end users. This decentralization reduces latency, increases speed, and also allows for improved bandwidth utilization. It also results in enhanced privacy and security since data do not have to traverse across the network, thereby reducing exposure [28].
  6. The SDN is an integral part of 5G network architecture, offering a programmable control plane that separates the network control and forwarding functions. This enables network administrators to manage traffic from a centralized console without needing to manipulate individual switches, thereby enhancing network flexibility and adaptability [29].
  7. The technical foundations of 5G telecommunications technology are built on a combination of innovative technologies and strategic improvements over the previous generations. These technological innovations form the core pillars of 5G and significantly contribute to its unique features, encompassing Enhanced Mobile Broadband (eMBB), URLLC, and mMTC [30].
  8. The eMBB caters to services and applications that demand high data rates across a large coverage area. It is designed to support scenarios requiring dense, high-volume, and high-speed data transfer, such as high-definition video streaming, virtual and augmented reality, and other immersive media applications. The technological prowess of eMBB extends to offering peak data rates of up to 20 Gbps, setting new benchmarks in mobile broadband speed and capacity [31]. This capability is achieved through a combination of high-frequency bands and advanced antenna techniques like massive MIMO, beamforming, and efficient modulation schemes.
  9. The URLLC aims to support mission-critical applications that demand stringent reliability and low latency. It is designed to offer an ultra-reliable communication service, ensuring a good success rate for data transmission within a specified latency. Typical latency requirements for URLLC applications are in the order of 1 millisecond or less, which is a significant improvement over the previous network generations. These performance attributes make URLLC ideally suited for time-critical applications such as autonomous vehicles, industrial automation, remote surgery, and other critical IoT applications [32].
  10. The mMTC: It is designed to support massive IoT deployments, enabling connectivity between an enormous number of devices per square kilometer. With mMTC, 5G

can handle a significantly higher density of connected devices compared to previous generations, allowing the seamless operation of a plethora of IoT devices [33]. This is crucial for applications such as smart cities, smart homes, environmental monitoring, and agriculture, among others. To manage this vast device connectivity, 5G networks incorporate advanced device management, power management, and signaling techniques to ensure the efficient use of network resources and maintain device battery life [34]. In addition, these technical components define the capabilities of 5G networks, enabling it to address a diverse range of use cases, applications, and services. These are not separate networks but are distinct aspects of the overall 5G architecture, each playing its part in forming the cohesive, high-performing network that is 5G.



**Figure 3.** Threat landscape of 5G networks [35].

### 2.2. Reliability and Integrity of 5G Services

5G networks are expected to enable and support an unprecedentedly wide range of applications, from autonomous vehicles and telemedicine to smart cities and industrial automation. Many of these applications involve mission-critical services where even minor service interruptions or data alterations can have potentially catastrophic consequences [36]. Therefore, the reliability and integrity of services delivered over 5G networks are of paramount importance. Reliability in the context of 5G refers to the network's ability to deliver a consistent level of service, without interruptions or significant fluctuations in performance, even under challenging conditions. This is crucial for applications such as telemedicine and autonomous driving, where a high level of service availability and low latency are required. Network reliability also extends to the network's resilience against malicious attacks or system failures, with the ability to rapidly recover and maintain core functions [37]. Integrity, on the other hand, pertains to the assurance that data transmitted over the network remain unaltered during transmission, whether by accidental errors or de-



liberate tampering [38]. Given the sensitive nature of the data handled by 5G applications, ensuring data integrity is fundamental. An example is in financial transactions, where even a small discrepancy can lead to substantial monetary loss, or in healthcare applications, where incorrect patient data can result in erroneous diagnoses or treatments. To ensure reliability and integrity, 5G networks should adopt robust security measures, including advanced encryption techniques, reliable error detection and correction mechanisms, secure routing protocols, and resilient network architectures. Techniques such as redundancy, fault tolerance, and real-time anomaly detection can enhance the reliability and integrity of 5G services. Moreover, leveraging AI and machine learning for proactive threat detection and response can further strengthen network resilience [39]. The interconnected world that 5G networks facilitate brings immense opportunities, but it also requires unwavering attention to the reliability and integrity of services, cementing these elements as key pillars in the development and operation of 5G networks.

### *2.3. The Sixth Generation: The Next Frontier in Wireless Communications*

The projected sixth generation of wireless communication systems, 6G, is expected to be more than just an incremental upgrade from its predecessor, 5G. It is predicted to usher in unprecedented speeds, lower latencies, and a level of connectivity and integration that the world has never seen [40]. Where 5G introduced the concepts of mMTC and URLLC, 6G is anticipated to amplify these features to a new level. Think of technologies such as holographic meetings, high-definition augmented and virtual reality, and ultra-connected smart cities. Moreover, terahertz frequencies, cell-free architectures, and satellite-network integration are other key expected features of 6G, making global coverage and space-to-ground communications possible [41].

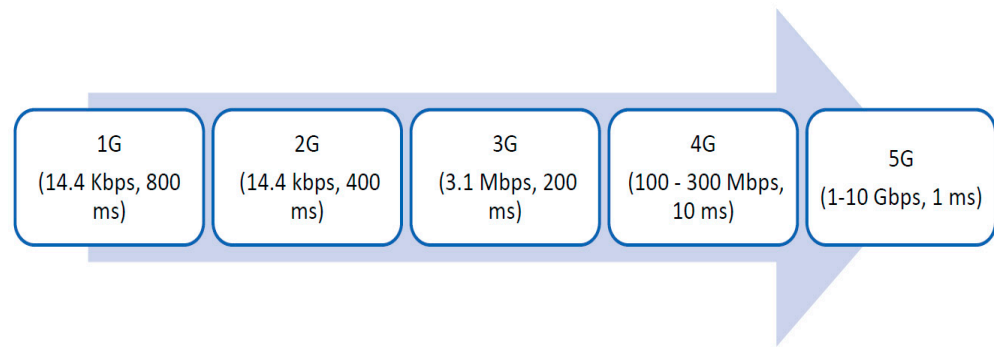
The potential of 6G is immense, but with that potential come significant security challenges. As the line between our physical and digital worlds becomes even more blurred, securing our wireless networks becomes not just a matter of data protection but a matter of personal safety [42]. Many researchers investigated 6G security and the use of AI and ML in enhancing 6G security [43,44]. However, with 6G networks being inherently AI-driven, the defense mechanisms will also rely heavily on artificial intelligence. AI can offer proactive threat detection, analyze vast datasets in real time to identify anomalies, and adapt dynamically to emerging threats [45]. However, this reliance on AI also brings vulnerabilities. There is a potential risk of adversaries manipulating AI operations, leading to system misbehaviors.

## **3. Mobile Network Security Evolution and the Evolution of Threat Landscape**

### *3.1. Evolution from 1G to 4G*

Mobile network security has evolved significantly from 1G to 5G networks. Each generation presented its unique security challenges influenced by technological advancements, changing user needs, and evolving threat patterns. Understanding this progression is crucial for addressing the demands of future 5G networks. In the 1980s, the 1G networks, providing analog voice services, had minimal security concerns [46]. However, with 2G's introduction of digital communication, the security landscape shifted. The digital nature of 2G made data vulnerable to interception and manipulation, prompting the introduction of encryption algorithms like A5/1, although some vulnerabilities like the A5/1 attacks still arose [47]. A graphical representation of mobile networks evolution is shown in Figure 4.

The 3G networks, which integrated broadband data services and IP-based services, opened the door to a wider range of threats, such as malware and phishing. To counteract these, robust encryption and mutual user–network authentication became necessary [48]. While, the fourth generation further expanded capabilities but also vulnerabilities, particularly with its all-IP network architecture [49]. This led to the development of sophisticated security measures, including advanced encryption and secure IP-based protocols. Thus, the evolution from 1G to 4G shows the interplay between technological evolution and escalating security focus.

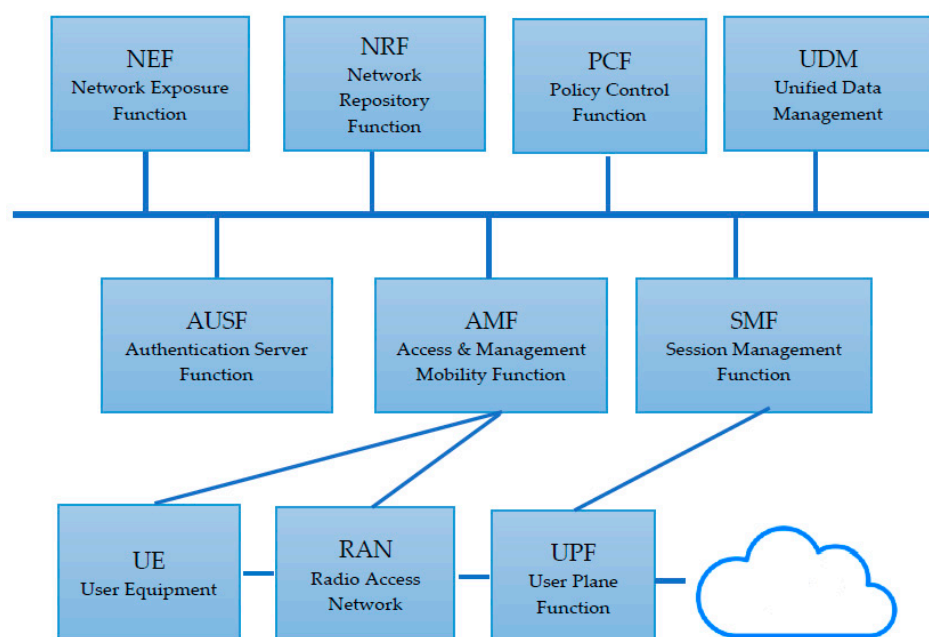


**Figure 4.** Evolution from 1G to 5G.

In addition, 3G’s integration with IP-based services brought both enhanced functionality and increased threats, prompting the use of more robust security measures. Further, 4G, emphasizing all-IP network architecture, brought even more vulnerabilities [50], requiring stronger countermeasures like advanced encryption and robust user authentication.

*3.2. Fifth-Generation Network Security*

With the advent of 5G telecommunications technology, there is an expanding proliferation of data transmission across vast digital landscapes. This significant shift in the realm of digital communications underscores the primacy of security in these next-generation networks. Security, in the context of 5G, encompasses multiple dimensions, from the privacy of personal information to the reliability and integrity of services offered through the network [51]. These elements have been a focal point in traditional networks; however, their importance is massively elevated in the 5G framework due to the inherent technical advancements and the larger, more diverse user-base that this technology caters to [52]. Fifth-generation networks, compared to their predecessors, are designed to handle a much broader range of applications, many of which involve the transmission of sensitive data and the delivery of critical services. Applications such as telemedicine, autonomous vehicles, and smart cities heavily rely on 5G networks for their operation, thereby escalating the need for robust and reliable security measures [53]. A summary of 5G security challenges is shown in Figure 5.



**Figure 5.** Fifth-generation architecture diagram.

Furthermore, the envisaged increase in machine-to-machine communications in the 5G era implies a shift in the nature of information being transmitted, with increased volumes of sensitive, operational data being communicated across networks [54]. The broadening of the attack surface, due to the increasing complexity of the network and the sheer number of connected devices, adds another layer of intricacy to the security landscape in 5G. The highly distributed architecture of 5G, combined with the heterogeneity of devices and services it supports, create multiple potential points of vulnerability that could be exploited by malicious entities. Ensuring the security of 5G networks, therefore, calls for a multifaceted approach that addresses not only the encryption and protection of data but also the secure management and authentication of devices and users [55]. The evolution towards the more connected world that 5G represents is closely intertwined with the need for more comprehensive and sophisticated security measures. Table 2 reports the most pressing security challenges encountered in the 5G landscape. Each challenge is corroborated by the pertinent literature, thereby providing a multifaceted understanding essential for both researchers and practitioners in the field. The table encapsulates areas such as network slicing vulnerabilities, authentication weaknesses, data privacy concerns, security issues in mMTC, edge computing security risks, man-in-the-middle attacks, and SDN risks.

**Table 2.** Fifth-generation security challenges.

5G Security Challenge	Citation(s)
Network slicing vulnerabilities	Mathew, A. (2020, March) [56], Wijethilaka, S.; Liyanage, M. (2021) [57], Salahdine, F., Liu, Q., Han, T. (2022) [58], Wu, T. Y., Jie, T. F. (2022) [59].
Authentication weaknesses	Basin, D., et al. (2018) [60]. Behrad, S., et al. (2019) [61], Sharma, et al. (2019) [62]. El Idrissi, et al. (2017) [63].
Data privacy concerns	Ahmad, I., et al. (2018) [6], Liyanage, M., et al. (2018) [64], Khan, R., et al. (2019) [4].
Security issues in mMTC	Hu, J., et al. (2022) [65], Chan, W. M., et al. (2023) [66], Salva-Garcia, P., et al. (2019) [67]
Edge computing security risks	Sha, K., et al. (2020) [68], Zhang, J., et al. (2018) [69], Xiao, Y., et al. (2019) [70], Sha, K., et al. (2020) [68]
Man-in-the-middle attacks in 5G	Conti, M., et al. (2016) [71], Kaplanis, C. (2015) [72], Mitev, M., et al. (2019) [73]
SDN Risks	Al Hayajneh, A., et al. (2020) [74], Hasneen, J., Sadique, K. M. (2022) [75]

Throughout the historical evolution of mobile networks, various strategies for securing these networks have been trialed, some proving to be more effective than others. The evaluation of these strategies offers valuable insights into the successful elements of security measures, as well as potential pitfalls to be avoided in the future. One of the significant successful strategies that have proven their effectiveness over time is the use of encryption. This is a measure that has been utilized since the advent of 2G networks, which transitioned from analog to digital data, thus increasing the risks of data interception and tampering. This led to the deployment of encryption algorithms, which have progressively become more sophisticated and robust as technology evolved from 2G to 4G [46,49].

Consequently, in 4G networks, advanced encryption standards were implemented, providing a significant level of protection for data. Another successful strategy has been the incorporation of mutual authentication between the user and the network. This strategy emerged in the 3G era and was carried over into 4G networks. Mutual authentication ensures that both the user and the network are legitimate, reducing the risk of unauthorized access and impersonation attacks. On the flip side, the transition from a traditional network architecture to an all-IP network architecture, particularly evident in 4G networks, has presented a significant pitfall [48,49]. While it facilitated higher data speeds and a seamless transition between different types of data services, it concurrently increased the network's attack surface. This heightened exposure to security threats like denial-of-service (DoS) and man-in-the-middle (MitM) attacks brought to light that the reliance on encryption and

authentication alone is not sufficient for ensuring network security [60,71]. This pitfall signaled the necessity for an integrated, multilayered approach to security, incorporating additional measures such as intrusion detection systems, firewalls, and anomaly detection technologies. The adoption of such an approach, initially in the 4G networks, revealed the value of these complementary measures in enhancing network security and addressing a broader range of threats.

However, there is an evolving role of encryption in countering threats: firstly, the encryption in 2G networks, where encryption made its notable debut during the 2G era, particularly focusing on ensuring data confidentiality during transmission. However, as our review uncovered, many of these early encryption protocols, like the A5/1 used in GSM, were susceptible to breaches as hackers grew more sophisticated [47]. Secondly, 3G and 4G encryption. With 3G and 4G, encryption techniques underwent a radical transformation. Smith and White elucidated how algorithms became more intricate, aiming to ensure not just confidentiality but also data integrity and authentication. The fourth generation, for instance, leveraged advanced encryption standards (AESs), which provided a robust defense against intrusions. This was a response to the increasingly complex software-based attacks that networks faced [76]. A comparison of the transformation in mobile network security and encryption strategies across generations is shown in Table 3.

Further, 5G encryption employs a multifaceted approach that leverages a variety of cryptographic techniques. For instance, the use of end-to-end encryption is now more prevalent, and in some instances, mandatory, in order to shield data from potential threats at all points of the transmission chain. Moreover, the inclusion of hardware-based security features like Trusted Execution Environments (TEEs) synergizes with cryptographic protocols to provide a fortified layer against physical and software-based attacks [77]. In addition, 5G aspires to be a harbinger of a new era in mobile network security, adopting a more comprehensive, layered, and agile encryption strategy to counter a broader array of threat vectors. This is evinced by the comparative analysis illustrated in Table 3, where the evolutionary trajectory of mobile network encryption strategies across generations is elucidated.

**Table 3.** 1G to 4G Security threats and encryption strategies [16,17,50,76,78,79].

Aspects	1G Networks	2G Networks	3G and 4G Networks
Nature of threats	Predominantly hardware-based vulnerabilities, such as physical tampering and unauthorized access.	Transition from analog to digital led to software-based threats.	Sophisticated software-based threats, including IP-specific attacks, due to transition to all-IP networks.
Typical threats	Frequency interference, eavesdropping, and unauthorized physical access.	Data interception, message tampering, and software vulnerabilities, such as buffer overflows.	Mobile malware, IP spoofing, phishing, man-in-the-middle attacks, and application-layer vulnerabilities.
Role of encryption	Minimal or absent; lack of standardized encryption protocols.	Introduction of encryption algorithms like A5/1 in GSM, albeit some were vulnerable.	Robust encryption standards such as AES and 3DES; enhanced focus on data integrity and user authentication.
Countermeasures	Physical security measures, such as locked cabinets and controlled access to network facilities.	Introduction of firewalls, intrusion detection systems (IDSs), and periodic security audits.	Multilayered security protocols, intrusion prevention systems (IPSs), real-time monitoring, and regular updates.

Table 3 offers an in-depth comparative analysis across mobile generations in terms of the nature of threats, typical threats encountered, role of encryption, and countermeasures adopted. In particular, the table highlights how threats have evolved from being predominantly hardware-based in 1G networks to increasingly sophisticated software-based attacks in 3G and 4G networks. Concurrently, encryption strategies have also undergone a

transformation: from minimal or absent standardized protocols in 1G to robust, multilayered encryption and security protocols in the latest generations. Countermeasures have similarly progressed, with a transition from rudimentary physical security approaches in 1G to real-time monitoring and multilayered security protocols in later generations.

### 3.3. Fifth-Generation Security Architecture

The security architecture of 5G networks is an intricate assembly designed to address the multifarious challenges brought forth by the next generation of connectivity (see Figure 5) [80]. The architecture is constructed on three pivotal components, each serving as a bulwark against specific sets of vulnerabilities and threats. In this section, we will expound upon each of these core components in greater detail.

#### 3.3.1. Authentication Framework

In 5G networks, the Authentication and Key Agreement (AKA) protocol serves as the cornerstone for secure communication. It has undergone substantial revisions compared to its 4G counterparts to address emerging security challenges: (1) Home network-based authentication: The authentication in 5G is primarily orchestrated by the home network rather than the serving network, a shift that eliminates several risks associated with rogue base stations. (2) SUPI (Subscription Permanent Identifier): A key feature introduced in 5G AKA is the use of SUPI. SUPI allows the home network to securely identify and authenticate a user, thereby creating an additional layer of security. (3) Extensibility: The AKA protocol in 5G is designed to be extensible, providing a framework that can adapt to future security requirements without necessitating a complete architectural overhaul [60,61].

#### 3.3.2. Network Slicing Security

The advent of network slicing is one of the defining features of 5G networks, allowing operators to create isolated “slices” of the network for different applications or services: (1) Isolation of slices: Each network slice operates as an autonomous entity with its own resources and network functions. This enables the implementation of slice-specific security policies. (2) Adaptive security measures: The security protocols can be tailored for each slice, accommodating varied requirements ranging from low-latency, high-reliability slices to slices designed for mMTC. (3) Resource allocation: The dynamic resource allocation capabilities of network slicing also extend to security resources, allowing for real-time adjustments in response to detected threats [56–59].

#### 3.3.3. Service-Based Architecture (SBA) Security

The fifth generation introduces the SBA, which radically departs from the hierarchical architectures seen in earlier generations: (1) Granular security controls: SBA allows for the application of security policies at a much finer granularity, made possible by its modular construction. Each service can be individually secured, which allows for enhanced flexibility in dealing with specific vulnerabilities. (2) Service-to-service communication: In SBA, services communicate through well-defined interfaces, often secured by contemporary security protocols like Transport Layer Security (TLS). This compartmentalization provides a more robust defense against potential attack vectors. (3) Decoupling of functions: The decoupling of network functions in SBA permits easier updates and modifications, thereby enabling quick responses to emerging security threats without affecting the overall network performance [81,82].

### 3.4. Implications for 5G Security

The security strategies of mobile networks have critical implications for the development and implementation of security measures in 5G networks. A primary implication drawn from the historical successes is the persistent need for strong encryption and authentication measures. Given the expanded connectivity, higher speeds, and increased volume of data associated with 5G, the importance of these fundamental security measures



is heightened. More than ever, users need to be assured of the integrity and confidentiality of their data. Consequently, 5G security architectures are expected to incorporate even more advanced encryption algorithms and multifactor authentication methods that are robust against emerging threats [6,37,51].

The pitfalls encountered during the evolution of mobile networks, notably during the transition to an all-IP network architecture in 4G, serve as a stark reminder of the importance of a holistic, multilayered approach to security [76]. Given the extensive connectivity, numerous devices, and diverse applications envisaged for 5G, the associated security challenges are even more complex [37,51]. It necessitates an integrated security approach that combines traditional measures like encryption and authentication with cutting-edge measures such as network slicing, AI and ML algorithms for anomaly detection, and advanced privacy-preserving techniques. Network slicing, for instance, allows the separation of different services onto individual network slices, thus isolating critical services and limiting the potential impact of a security breach [66]. AI and ML algorithms can be employed to learn normal network behaviors, identify anomalies that could signal a potential security threat, and initiate appropriate responses [37]. Advanced privacy-preserving techniques can provide better protection for user data, addressing the ever-growing concerns over data privacy in the age of the IoT and big data. Another critical implication is the need for adaptability and continuous evolution of security measures to respond to the ever-changing threat landscape. Fifth-generation networks, given their extensive connectivity and diverse applications, are expected to face new and potentially unforeseen security threats [6,51]. This necessitates proactive measures that can quickly identify, respond to, and neutralize such threats, demonstrating the need for dynamic, adaptive, and self-learning security systems.

#### 4. Security Threat Landscape in 5G Networks

##### 4.1. Evolution of Threat Landscape

The evolution of mobile networks from 1G to 5G technology presents an expanded threat landscape due to the network's complexity, enhanced functionalities, and the array of devices connected to it. As networks have become more sophisticated, so too have the potential threats [46]. The shift from 2G's digital framework to 3G's IP-based services expanded the threat landscape to include issues such as malware and phishing [50]. The advent of 4G, with its all-IP structure, heightened vulnerability to IP-specific attacks like DoS and MitM attacks. The decentralized, software-driven architecture of 5G further amplifies these risks, introducing advanced cyber threats related to edge computing and supply chain vulnerabilities. The large-scale integration of IoT devices into 5G networks also increases the potential for botnet attacks and data privacy breaches [68].

In addition, security measures have adapted over time. Basic techniques like frequency hopping were sufficient for addressing 1G's primary concerns of eavesdropping and unauthorized access. The introduction of encryption algorithms in 2G provided a foundational layer of security, which had to be further reinforced in 3G through robust encryption and mutual authentication mechanisms. The complex threat environment of 4G required even stronger measures, incorporating advanced technologies like machine learning for anomaly detection [50,76]. ENISA [35], the European Union's cybersecurity arm, released a threat landscape report for 5G networks, evaluating the risks associated with the fifth generation of mobile communication networks (5G), as shown in Figure 3.

##### 4.2. Threat Landscape in 5G Networks

There are a number of key areas of concern within the 5G security landscape. First and foremost is the threat of cyberattacks, with the aim of either disrupting network operations or gaining unauthorized access to sensitive data. Cyberattacks can take many forms, from distributed denial-of-service (DDoS) attacks, which aim to overwhelm network resources and disrupt services, to advanced persistent threats (APTs), which are long-term targeted attacks that seek to remain undetected while siphoning off data or damaging

network operations [83]. Another area of concern in 5G networks is the threat to user privacy. With an increased amount of data being transferred and processed, there is a corresponding increase in the risk of unauthorized data access or leakage [64]. Given the range of services and applications running on 5G networks, from IoT devices to mission-critical communications, ensuring the privacy of user data is of paramount importance. Further, the enhanced capabilities of 5G networks, such as network slicing and the use of edge computing, while offering significant benefits, can also introduce new security vulnerabilities [56,57]. For instance, the virtualization of network functions may open up new vectors for cyberattacks. Meanwhile, the use of edge computing, while reducing latency, may increase the attack surface by distributing data processing and storage across numerous devices and locations [68,69].

Table 4 encapsulates this evolutionary path, identifying the key security threats and features pertinent to each mobile network generation. Initial 1G networks were focused mainly on analog voice services, offering a somewhat insular threat landscape that chiefly included risks like eavesdropping. The digital revolution heralded by 2G prompted novel security concerns related to data interception but also marked the debut of encryption algorithms such as A5/1 as a countermeasure. The introduction of broadband and IP-based services in 3G extended the threat landscape to include malware, phishing, and data leakage, counterbalanced by enhanced security features like robust encryption and mutual authentication. With 4G's all-IP network structure, the threats evolved to include DoS, MitM, and data sniffing attacks, necessitating advanced security measures such as stronger encryption algorithms and firewalls. Lastly, 5G presents a decentralized, software-driven architecture, introducing a panoply of advanced cyber threats ranging from edge computing vulnerabilities to large-scale botnet attacks. This complexity is met with equally sophisticated countermeasures, including zero-trust architecture and AI-based anomaly detection.

**Table 4.** The evolution of the threat landscape from 1G to 5G networks [35,78,79].

Generation	Threat Landscape and Security Features
1G	Primarily focused on analog voice services, leading to limited security concerns. Risk of eavesdropping due to the lack of encryption.
2G	Transition to digital communication led to data interception threats. Security measures include encryption algorithms such as A5/1 to counteract these risks.
3G	Introduction of broadband and IP-based services expanded the threat landscape to include malware, phishing, and data leakage. Security enhancements like robust encryption and mutual authentication were deployed.
4G	All-IP network structure brought new threats like DoS, MitM, and data sniffing attacks. Advanced security measures such as stronger encryption algorithms and firewalls were introduced.
5G	Decentralized and software-driven architecture gives rise to advanced cyber threats, including edge computing vulnerabilities and supply chain attacks. IoT integration amplifies risks like large-scale botnet attacks and data privacy breaches. Countermeasures include zero-trust architecture and AI-based anomaly detection.

#### 4.3. Fifth-Generation Network Potential Vulnerabilities

The versatile and advanced features of 5G networks, while propelling significant improvements in terms of connectivity, speed, and user experience, simultaneously pave the way for a multitude of potential vulnerabilities. These vulnerabilities, due to the broad attack surface and the complexity of the 5G system, can emerge at various layers and interfaces of the network.

**Device-level vulnerabilities:** The anticipated explosion of connected devices, particularly under the proliferation of the IoT in the 5G era, inherently expands the attack surface. Each connected device, ranging from smart home appliances to industrial sensors, represents a potential point of vulnerability. The security protocols of these devices, often

low-powered and with minimal security features, can be exploited by malicious entities, thus allowing unauthorized access into the network [84].

**Software and virtualization vulnerabilities:** The shift towards SDN and NFV in 5G networks, while improving network flexibility and management, opens new potential security holes. The possibility of software bugs, misconfigurations, and the lack of physical control over virtualized functions could lead to security breaches. Furthermore, these centralized functions could present single points of failure, where compromises can have widespread effects [74,75].

**Network slicing vulnerabilities:** Although network slicing provides a platform for customized and isolated services, it also introduces security risks. An adversary gaining access to one network slice could exploit inter-slice vulnerabilities, affecting other slices and possibly leading to cross-slice attacks. Therefore, securing slice isolation becomes critical [56–59].

**Edge computing vulnerabilities:** While edge computing provides benefits in terms of latency and bandwidth utilization, it also places data and computation closer to potential attack points. This shift exposes the network to additional local breaches and data leaks, mandating advanced security solutions at the edge [68–70].

**Radio interface vulnerabilities:** The use of new radio technologies such as massive MIMO and mmWave can introduce vulnerabilities related to signal interception and jamming. Also, these technologies, while improving network capacity and speed, could potentially be exploited to launch DoS attacks [84,85].

**Supply chain vulnerabilities:** The global and complex nature of the 5G supply chain can present significant security risks. The compromise of hardware or software at any point in the supply chain, such as the inclusion of malicious code or the installation of hardware backdoors, can lead to widespread network vulnerabilities [80]. Table 5 provides a summary of the key security threats in 5G networks, their potential impacts, and specific attack methods and techniques [85,86].

**Table 5.** Summary of the key security threats in 5G networks, their potential impacts, and attack methods and techniques.

Security Threat	Description	Potential Impact	Attack Methods and Techniques
Cyberattacks [83,87]	Threats aimed at disrupting network operations or gaining unauthorized access to sensitive data, including DDoS attacks and APTs.	Network disruption, data breaches, service degradation.	DDoS attacks leveraging higher bandwidth in 5G. APTs using techniques like social engineering, zero-day exploits, and rootkits.
User privacy [4,6,64]	Risk of unauthorized data access or leakage due to increased data transfer and processing on 5G networks.	Data breaches, privacy violations, identity theft.	Unauthorized data access or eavesdropping. Data leakage through insecure channels.
Security vulnerabilities [56–59,74,75,84–86]	5G’s capabilities like network slicing and edge computing introduce new vulnerabilities. Virtualized network functions and data distribution can be exploited.	Network compromise, data breaches, system instability.	Exploiting virtualized network function vulnerabilities. Unauthorized access via edge computing devices. Targeting insecure network slices.
IoT devices [68,71–74,88]	Proliferation of IoT devices with weak security can be targeted to compromise the network or for unauthorized data access.	Botnet creation, network compromise, data theft.	Creating botnets through vulnerable IoT devices. Exploiting weak IoT security. Unauthorized access via compromised IoT devices.

Table 5. Cont.

Security Threat	Description	Potential Impact	Attack Methods and Techniques
Cloud services and edge computing [68–70]	Enhancing performance but expanding the attack surface by distributing data processing and storage.	Data breaches, service disruption, unauthorized access.	Targeting cloud vulnerabilities. Unauthorized access via edge computing devices. Attacks against distributed cloud services.
SDN and NFV [89–91]	Decentralization and virtualization create new attack points.	Network compromise, data breaches, system instability.	Exploiting SDN vulnerabilities. Targeting NFV infrastructure. Unauthorized access through virtualization.
Network slicing [56–59]	Enhances security through compartmentalization. However, poor slice isolation or misconfigurations can lead to risks.	Unauthorized access, lateral movement, data breaches.	Exploiting misconfigured network slices. Unauthorized access through vulnerable slices. Lateral movement between slices.
Potential attackers [87,92]	Threats from cybercriminals, state-sponsored attackers, or insiders (like employees).	Varied, based on attacker objectives.	Cybercriminal tactics like malware, ransomware, DDoS. APT techniques like zero-days, rootkits. Insider threats exploiting or misusing access.
Attack methods [5,71–73,83,89,93]	Methods like DDoS due to higher bandwidth, man-in-the-middle attacks via IoT and edge computing, APTs, and software vulnerabilities from SDN and NFV.	Diverse, based on method.	DDoS attacks to overwhelm resources. Man-in-the-middle attacks for data interception. APTs for prolonged access. Exploiting SDN and NFV software vulnerabilities.

Table 5 delineates the key security threats in 5G networks, offering a comprehensive description of each threat, its potential impact, and prevalent attack methods and techniques. The threats range from cyberattacks aimed at disrupting network operations to potential vulnerabilities inherent in 5G's capabilities like network slicing and edge computing. Other notable concerns include the proliferation of the IoT devices with weak security and the enhanced attack surface resulting from the adoption of cloud services [94]. Decentralization and virtualization technologies like SDN and NFV further amplify the risks. Moreover, the diversity of potential attackers—from cybercriminals to state-sponsored entities—adds another layer of complexity.

#### 4.4. Anticipated Threat Vectors

As 5G networks continue to evolve, they introduce new and increasingly sophisticated threat vectors. These encompass not just the malicious actors and their methods but also the system vulnerabilities they may exploit [51,78,79]. A comprehensive understanding of these anticipated threat vectors in the 5G landscape is crucial for developing effective security measures. One of the most significant anticipated threat vectors in 5G networks is the proliferation of IoT devices. These devices often have limited computational resources and weak security features, making them attractive targets for cyber attackers. Once compromised, these devices can be used as stepping stones to launch larger-scale attacks on the network or to gain unauthorized access to sensitive data [68,71–74]. Another anticipated threat vector in 5G networks is the expanded use of cloud services and edge computing [94,95]. While these technologies increase network flexibility and performance, they also expand the attack surface by distributing data processing and storage across numerous devices and locations. This can create new vulnerabilities and increase the complexity of securing the network [68,70]. SDN and NFV, key elements of 5G architecture, are also potential threat vectors. These technologies decentralize network control and

introduce virtualization layers, potentially creating new points of attack for cybercriminals. Finally, network slicing, another central feature of 5G, can be a potential threat vector. While network slicing can enhance security through compartmentalization, poor slice isolation or misconfigurations can result in security risks, allowing malicious actors to exploit one slice to gain access to others [89–91]. Understanding these anticipated threat vectors in the 5G environment is the first step towards developing proactive and comprehensive security measures that can address these challenges.

#### *4.5. Potential Attackers and Their Motivations*

Understanding the potential attackers in the 5G environment and their motivations is a critical step in identifying and mitigating potential threats. Potential attackers in the context of 5G may be categorized into three broad groups, based on their capabilities, objectives, and the resources at their disposal: cybercriminals, state-sponsored attackers, and insider threats [71,87]. Cybercriminals typically launch attacks with the aim of achieving financial gain. These actors employ a range of methods to compromise 5G networks, including malware, ransomware, and DDoS attacks. They often exploit weak security controls, insecure interfaces, and poor user security practices [87]. State-sponsored attackers or APTs represent a significant threat to 5G networks due to their high level of sophistication and the substantial resources at their disposal. Their motivations may include espionage, disruption of critical infrastructure, or gaining a competitive advantage at a national level. These attackers often utilize advanced techniques to evade detection, remain persistent within the network, and achieve their objectives [72,87]. Insider threats, although often overlooked, can pose a substantial risk to 5G security. Disgruntled employees, contractors with access to sensitive network information, or even employees unwittingly manipulated by external actors, can cause significant damage to network security. These attacks can be particularly challenging to detect and mitigate due to the inherent trust placed in these individuals. In order to effectively mitigate these threats, it is critical that security measures account for the various attackers' capabilities, strategies, and motivations and that they are adaptable to evolving threat landscapes.

#### *4.6. Attack Methods and Techniques*

As 5G networks become increasingly sophisticated, so do the methods and techniques used by potential attackers to exploit vulnerabilities. A few of the anticipated attack methods and techniques are outlined in this section. The DDoS attacks are anticipated to be a significant threat to 5G networks. As 5G networks offer significantly higher bandwidth, they could potentially be leveraged to launch larger-scale DDoS attacks than those seen on previous generations of mobile networks [89,93]. Another anticipated method is the MitM attack, where an attacker intercepts communication between two parties to steal data or inject malicious content. The increased reliance on edge computing and IoT devices, which often have weaker security measures, makes 5G networks potentially more vulnerable to MitM attacks [96]. The APTs are another anticipated attack method in 5G networks. These sophisticated attacks are often state-sponsored and involve a prolonged and targeted effort to compromise a network. APTs often employ a mix of attack techniques, including social engineering, zero-day exploits, and rootkits to gain access and maintain a foothold in the target network [97]. Finally, the exploitation of software vulnerabilities is an anticipated attack method in 5G networks. The shift towards SDN and NFV in 5G introduces a new attack surface, as attackers may seek to exploit vulnerabilities in the software layers [89–91]. Understanding these attack methods and techniques is crucial for developing effective countermeasures and securing 5G networks.

#### *4.7. Analysis of Inherent Vulnerabilities in Network Slicing*

Network slicing is a critical feature of 5G networks, enabling operators to create multiple virtual networks on a single physical infrastructure. While this feature brings numerous benefits, such as customizability, scalability, and efficient resource utilization, it also in-



roduces new vulnerabilities and amplifies the potential impact of security breaches [56]. One significant vulnerability lies in the inherent complexity of managing multiple virtual networks concurrently. Each slice may serve different applications and services, having its own unique security requirements and configuration. Managing these complex configurations and maintaining isolation between slices is challenging, and any misconfiguration or overlap could lead to breaches and leakage of sensitive information across slices [57,58]. The orchestration process is another vulnerability in network slicing. Orchestrators are responsible for the allocation and management of resources across slices. An attacker compromising the orchestrator could control resource allocation, potentially leading to the unauthorized access of network slices or DoS attacks on specific slices. Inter-slice communication is yet another vulnerability. Although slices are designed to be isolated, communication between slices can occur. If the security protocols governing these interactions are not robust, an attacker could exploit this communication to launch attacks on different slices.

The dependence on SDN and NFV for implementing network slicing also introduces vulnerabilities. SDN and NFV architectures could potentially be exploited if they contain software vulnerabilities or are misconfigured [89,90].

The technical aspects of network slicing, while enabling greater flexibility and optimization, also introduce potential weaknesses. Network slicing necessitates a more dynamic, programmable, and software-based environment, primarily facilitated by SDN and NFV. While these technologies provide flexibility and optimization capabilities, they also introduce software vulnerabilities that may be exploited by attackers [57,59]. The isolation between network slices is another crucial technical aspect. Each network slice is envisioned to operate independently of the others, providing services tailored to its specific use case. However, maintaining robust isolation and preventing interference between network slices is technically challenging. Misconfigurations or software vulnerabilities could compromise the isolation, potentially enabling an attacker to gain access to multiple slices or causing interference between slices [55,58,84]. The inherent vulnerabilities in network slicing in 5G networks and their associated mitigation strategies are outlined in Table 6.

**Table 6.** Vulnerabilities in network slicing in 5G networks and their associated mitigation strategies [56–59].

Vulnerability	Potential Impact	Exploitation Techniques	Mitigation Strategies
Complex slice configurations	Breaches, data leakage, security risks	<ul style="list-style-type: none"> <li>- Configuration errors</li> <li>- Weak access controls</li> <li>- Inadequate security protocols</li> </ul>	<ul style="list-style-type: none"> <li>- Develop robust security protocols for inter-slice communication.</li> <li>- Implement stringent configuration management practices.</li> <li>- Regularly audit and assess slice configurations for vulnerabilities.</li> </ul>
Orchestration vulnerabilities	Unauthorized resource access, DoS attacks, security breaches	<ul style="list-style-type: none"> <li>- Weak authentication</li> <li>- Unauthorized access to orchestrator interfaces</li> <li>- Exploiting vulnerabilities in orchestrator software</li> </ul>	<ul style="list-style-type: none"> <li>- Harden orchestrator security with strong authentication and access controls.</li> <li>- Implement anomaly detection mechanisms to identify suspicious orchestrator activities.</li> <li>- Regularly update and patch orchestrator software.</li> </ul>

Table 6. Cont.

Vulnerability	Potential Impact	Exploitation Techniques	Mitigation Strategies
Inter-slice communication	Data breaches, unauthorized access	<ul style="list-style-type: none"> <li>- Lack of encryption</li> <li>- Insufficient authentication</li> <li>- Exploiting vulnerabilities in communication protocols</li> </ul>	<ul style="list-style-type: none"> <li>- Strengthen inter-slice communication security with encryption and authentication.</li> <li>- Implement intrusion detection systems to monitor inter-slice traffic for anomalies.</li> <li>- Restrict unnecessary communication between slices.</li> </ul>
SDN and NFV vulnerabilities	Network compromise, data breaches, system instability	<ul style="list-style-type: none"> <li>- Unpatched vulnerabilities in SDN/NFV components</li> <li>- Misconfigurations in SDN/NFV controllers and switches</li> <li>- Unauthorized access to SDN/NFV management interfaces</li> </ul>	<ul style="list-style-type: none"> <li>- Regularly update and patch SDN and NFV software components.</li> <li>- Perform rigorous security testing and audits of SDN and NFV infrastructure.</li> <li>- Implement secure configurations and access controls.</li> </ul>
Resource allocation weaknesses	Service disruptions, resource monopolization, security breaches	<ul style="list-style-type: none"> <li>- Unauthorized access to resource allocation mechanisms</li> <li>- Manipulating resource allocation policies</li> <li>- Resource allocation based on weak criteria</li> </ul>	<ul style="list-style-type: none"> <li>- Implement robust authentication and authorization mechanisms for resource allocation. Monitor resource allocation for unusual patterns or anomalies.</li> <li>- Employ intrusion detection systems to detect and respond to resource allocation attacks.</li> </ul>

In Table 6, the complex landscape of vulnerabilities inherent in 5G network slicing is succinctly elucidated, categorizing each vulnerability by its potential impact, exploitation techniques, and recommended mitigation strategies. The table underscores the need for robust security protocols and stringent configuration management practices in dealing with complex slice configurations. It also highlights the urgency for securing orchestration interfaces and implementing strong authentication mechanisms. Additionally, vulnerabilities tied to SDN and NFV are indicated, necessitating regular software updates and rigorous security audits. The table serves as a comprehensive guide for understanding and addressing the multifaceted security challenges in 5G network slicing.

#### 4.8. Risk Considerations in mMTC

mMTC is one of the critical use cases envisioned for 5G networks, facilitating communication between a large number of devices in applications such as smart cities, industrial automation, and the IoT. While mMTC brings significant potential for various applications, it also introduces several unique security risks [65]. One fundamental risk consideration is the vast number of devices involved in mMTC. The sheer quantity of devices exponentially increases the attack surface for potential attackers. Each device represents a potential entry point for attackers, which could be exploited to gain unauthorized access to the network or launch DoS attacks.

The heterogeneity of devices in mMTC scenarios also poses a risk. Devices in an mMTC environment can vary significantly in terms of their capabilities, security features, and vulnerabilities. Ensuring the security of all these diverse devices can be challenging, as the weakest device could potentially be exploited to compromise the entire network. Furthermore, the requirement for low latency and high reliability in mMTC introduces potential security risks [65]. The need for timely communication between devices can make it challenging to implement robust security measures, such as complex encryption algorithms, without causing unacceptable delays or affecting reliability. These unique risk

considerations necessitate the development of tailored security measures for mMTC in 5G networks [66].

#### 4.9. New Challenges and Threats

The advent of mMTC in 5G networks brings forth new challenges and threats. Primarily, the massive increase in device connections leads to an enormous volume of data transmission, leading to higher network congestion [65]. This can potentially be exploited by malicious entities for DDoS attacks. Another challenge arises due to the resource-constrained nature of many mMTC devices. They often operate on limited power and computational resources, making it challenging to deploy robust security measures like advanced encryption and real-time monitoring [66]. As a result, these devices can be more vulnerable to various security threats, including device spoofing, man-in-the-middle attacks, and data breaches. Device heterogeneity further complicates the security landscape, as a multitude of device types, with varying levels of security, try to interact within the same network. This situation can lead to inconsistent security measures, creating weak points that can be exploited by attackers [67].

Further, the need for low-latency communication in many mMTC applications can conflict with the implementation of robust security measures. Security processes such as encryption, authentication, and intrusion detection can introduce delays, potentially compromising the performance of time-sensitive applications [66]. These new challenges and threats necessitate novel approaches to security in mMTC, balancing the need for robust security measures with the unique constraints and requirements of mMTC applications in 5G networks [67].

#### 4.10. Security Solutions for mMTC

As the risk landscape for mMTC in 5G networks is complex, securing these networks requires innovative solutions. Research and developments in this domain have centered on several key strategies, as shown in Table 7. One of the strategies involves using lightweight cryptographic methods suitable for resource-constrained devices. Such methods aim to secure data transmission without overly burdening the device's computational and power resources. For example, symmetric encryption algorithms, such as the advanced encryption standard (AES), can offer a balance between security and computational efficiency [66].

**Table 7.** Security solutions for mMTC in 5G networks [65–67].

Security Solutions for mMTC	Description	Advantages	Challenges	Use Cases
Lightweight cryptographic methods	Utilizes lightweight cryptographic techniques suitable for resource-constrained mMTC devices. Aims to secure data transmission without imposing a significant computational or power burden.	<ul style="list-style-type: none"> <li>- Minimizes computational and power overhead.</li> <li>- Suitable for devices with limited resources.</li> </ul>	<ul style="list-style-type: none"> <li>- May provide lower levels of security compared to heavier encryption methods.</li> </ul>	<ul style="list-style-type: none"> <li>- Secure data transfer in mMTC devices with limited resources.</li> </ul>
Distributed security mechanisms	Implements distributed security mechanisms where the security workload is shared among multiple devices or network nodes. It prevents a single point of failure and is particularly effective against DoS and DDoS attacks.	<ul style="list-style-type: none"> <li>- Enhanced resilience against attacks.</li> <li>- Effective in preventing network congestion due to attacks.</li> </ul>	<ul style="list-style-type: none"> <li>- Requires coordination among multiple devices or nodes.</li> <li>- Complex to implement and manage.</li> </ul>	<ul style="list-style-type: none"> <li>- Protection against DoS and DDoS attacks in mMTC networks.</li> </ul>
Intrusion detection systems (IDSs)	Utilizes IDS to monitor network traffic and identify suspicious activities. It plays a critical role in the timely detection and mitigation of potential threats in mMTC environments.	<ul style="list-style-type: none"> <li>- Provides real-time threat detection.</li> <li>- Alerts network administrators to potential security breaches.</li> </ul>	<ul style="list-style-type: none"> <li>- May generate false positives.</li> <li>- Requires constant monitoring and updates.</li> </ul>	<ul style="list-style-type: none"> <li>- Early detection of security threats in mMTC applications.</li> </ul>

Table 7. Cont.

Security Solutions for mMTC	Description	Advantages	Challenges	Use Cases
Intrusion prevention systems (IPSs)	Implements IPS to proactively block or prevent detected security threats. It enhances the security posture of mMTC networks by stopping potential attacks before they can cause harm.	<ul style="list-style-type: none"> <li>- Actively prevents security threats from causing damage.</li> <li>- Reduces the impact of security incidents.</li> </ul>	<ul style="list-style-type: none"> <li>- Possibility of false positives and false negatives.</li> <li>- Requires regular updates and fine-tuning.</li> </ul>	<ul style="list-style-type: none"> <li>- Proactive security measures for mMTC networks.</li> </ul>
Machine learning (ML) and artificial intelligence (AI)	Harnesses machine learning (ML) and artificial intelligence (AI) techniques to analyze vast amounts of network data. It is adept at identifying patterns and anomalies, greatly enhancing the ability to detect and prevent cyberattacks in mMTC networks.	<ul style="list-style-type: none"> <li>- Adaptive and self-learning capabilities.</li> <li>- Effective in identifying complex attack patterns.</li> </ul>	<ul style="list-style-type: none"> <li>- Requires extensive training and data.</li> <li>- May generate false positives without proper tuning.</li> </ul>	<ul style="list-style-type: none"> <li>- Advanced threat detection and prevention in mMTC networks.</li> </ul>
Rigorous authentication mechanisms	Deploys rigorous authentication mechanisms to ensure that only authorized devices and entities can access the mMTC network. Access control measures are employed to prevent unauthorized access to the network and sensitive data.	<ul style="list-style-type: none"> <li>- Ensures only trusted devices access the network.</li> <li>- Protects sensitive data from unauthorized access.</li> </ul>	<ul style="list-style-type: none"> <li>- May introduce latency in the authentication process.</li> <li>- Requires robust management of authentication credentials.</li> </ul>	<ul style="list-style-type: none"> <li>- Secure access control in mMTC applications.</li> </ul>

Distributed security mechanisms represent another approach, where the security workload is shared among multiple devices or network nodes. This approach can prevent a single point of failure and can be particularly effective against DoS and DDoS attacks [51]. Intrusion detection systems (IDSs) and IPS also have a role to play in securing mMTC. These systems can monitor network traffic and identify suspicious activities, allowing for the timely detection and mitigation of potential threats. AI algorithms have shown promise in improving security in mMTC. These techniques can analyze vast amounts of network data to identify patterns and anomalies, helping to detect and prevent cyberattacks. In addition, strict authentication and access control mechanisms are crucial for securing mMTC in 5G networks. They can prevent unauthorized devices from gaining access to the network or accessing sensitive data [67].

Table 7 offers an in-depth exploration of security solutions tailored for mMTC in 5G networks. It delineates various approaches from lightweight cryptographic methods designed for devices with limited computational resources to more sophisticated solutions like machine learning and artificial intelligence for anomaly detection. Each approach is scrutinized for its advantages and challenges, providing insights into their applicability under specific use cases. Lightweight cryptographic methods, for instance, minimize power and computational overhead but may compromise on the level of security provided. Distributed security mechanisms enhance resilience against attacks such as DoS and DDoS but necessitate complex coordination among devices or nodes. Intrusion detection and prevention systems offer real-time threat monitoring and proactive defenses but require frequent updates and may generate false positives. Machine learning and AI-based solutions stand out for their adaptive capabilities but require extensive training data.

#### 4.11. Analysis of 5G Security Challenges in Conjunction with Edge Computing

The integration of edge computing into 5G networks enhances performance through reduced latency and increased capacity for real-time data processing. However, this shift also brings new security challenges.

Firstly, the decentralization of data processing, inherent to edge computing, increases the number of attack vectors. The data are processed closer to the user, which expands the potential points of attack and increases the complexity of implementing centralized security measures [68]. Moreover, edge nodes are often less powerful than centralized

servers in terms of computational capacity, making them potentially more vulnerable to cyberattacks. Deploying robust security measures on edge nodes can be challenging due to these resource limitations. Furthermore, edge computing's dependency on the IoT devices, which are known for their diverse security levels and standards, adds another layer of complexity to the security challenges [69]. This diversity often results in an inconsistent security landscape, which can be exploited by attackers. Privacy is also a concern with edge computing in 5G networks. Data are processed closer to the user device, making it more vulnerable to breaches if not adequately protected.

The potential risks and vulnerabilities in edge computing within 5G networks are multifaceted, resulting from various factors, such as the increased number of devices, decentralization of data processing, and lack of uniform security standards. Edge computing dramatically increases the number of devices involved in data processing and communication, each representing a potential point of entry for attackers. The heterogeneous nature of these devices further complicates the security landscape, as different devices might have different vulnerabilities [70]. Data integrity is another major concern. The decentralization of data processing means that data might travel through various nodes before reaching its destination, increasing the risk of data corruption or manipulation. Additionally, edge computing environments often lack the physical security measures present in traditional data centers, making them susceptible to physical attacks. Compromised hardware could lead to the loss or theft of sensitive data. Moreover, the heterogeneity of edge devices often results in a lack of uniform security protocols and standards. This inconsistency can be exploited by attackers to launch cyberattacks, such as DDoS attacks or malware infection [70].

Implementing robust protective measures in edge computing is critical to secure the operations of 5G networks. The mitigation strategies should take into account the unique challenges of edge computing, including the high number of devices, the decentralized data processing, and the inconsistency of security protocols among devices. Firstly, as edge computing expands the surface area for potential attacks, perimeter defense strategies must be upgraded to be more dynamic and responsive. This includes utilizing machine learning algorithms for threat detection and mitigation, which can adapt and respond to emerging threats in real time [68]. Secondly, the concept of "security by design" should be implemented in edge computing environments. This approach involves integrating security measures at every stage of system design and operation, rather than applying them as an afterthought. Moreover, data encryption should be applied to ensure the integrity and confidentiality of data, preventing unauthorized access and manipulation. It is essential to deploy robust encryption mechanisms to secure the communication between edge devices and central nodes. Additionally, the standardization of security protocols across edge devices can enhance their resilience against cyberattacks in edge applications. Establishing industry-wide standards for edge security would help create a more unified and less vulnerable security landscape. Further, a summary of the security challenges in edge computing in 5G, along with potential risks, vulnerabilities, and protective measures, is displayed in Table 8.

**Table 8.** Fifth-generation security challenges and edge computing: potential risks, vulnerabilities, and protective measures [68–70].

Security Challenges in Edge Computing in 5G	Potential Risks and Vulnerabilities	Protective Measures
Decentralization of data processing	<ul style="list-style-type: none"> <li>- Increased attack vectors due to processing data closer to users.</li> <li>- Edge nodes with lower computational capacity are more vulnerable.</li> </ul>	<ul style="list-style-type: none"> <li>- Upgrade perimeter defense strategies to be dynamic and responsive.</li> <li>- Implement machine learning for real-time threat detection and mitigation.</li> <li>- Apply "security by design" principles in system design and operation.</li> </ul>



Table 8. Cont.

Security Challenges in Edge Computing in 5G	Potential Risks and Vulnerabilities	Protective Measures
Dependency on IoT devices	<ul style="list-style-type: none"> <li>- Diverse security levels and standards among IoT devices.</li> <li>- Inconsistent security landscape that can be exploited.</li> </ul>	<ul style="list-style-type: none"> <li>- Standardize security protocols across edge devices for a more uniform security landscape.</li> <li>- Establish industry-wide security standards for edge computing.</li> </ul>
Data privacy concerns	<ul style="list-style-type: none"> <li>- Data processed closer to user devices increases vulnerability to breaches.</li> </ul>	<ul style="list-style-type: none"> <li>- Implement robust data encryption mechanisms to ensure integrity and confidentiality.</li> <li>- Secure communication between edge devices and central nodes with strong encryption.</li> </ul>
Increased number of devices	<ul style="list-style-type: none"> <li>- More devices involved, each representing a potential entry point for attackers.</li> </ul>	<ul style="list-style-type: none"> <li>- Upgrade perimeter defense strategies.</li> <li>- Utilize machine learning for real-time threat detection and response.</li> </ul>
Data integrity risks	<ul style="list-style-type: none"> <li>- Data travel through various nodes, increasing the risk of corruption or manipulation.</li> </ul>	<ul style="list-style-type: none"> <li>- Implement data encryption to prevent unauthorized access and manipulation.</li> </ul>
Physical security vulnerabilities	<ul style="list-style-type: none"> <li>- Lack of physical security measures in edge computing environments.</li> <li>- Compromised hardware could lead to data loss or theft.</li> </ul>	<ul style="list-style-type: none"> <li>- Implement strong access controls and monitoring systems to prevent physical tampering of edge devices.</li> </ul>

Table 8 outlines the security challenges inherent to the integration of edge computing within 5G networks. It identifies key risks such as increased attack vectors due to data decentralization, varied security standards in IoT devices, and data integrity concerns. Each challenge is paired with recommended protective measures like robust encryption, machine learning for threat detection, and industry-wide security standardization.

#### 4.12. Security Breaches in 5G Networks

Investigating past breach events is crucial to understand the vulnerabilities in 5G networks and formulate robust security measures. This section delves into an analysis of notable breach events, focusing on the type of attack, tactics utilized by attackers, the network's vulnerabilities exploited, and the resulting implications. One of the significant breach events in recent history involved exploiting the vulnerabilities of the 5G AKA protocol [96]. There exists a notable instance where attackers exploited the 5G AKA protocol, which led to an MitM attack [71]. In this breach event, the attackers intercepted and altered the communication between two parties, resulting in unauthorized access to sensitive data and causing considerable disruption to the network's operations. Furthermore, DDoS attacks have also been responsible for significant security breaches in 5G networks. This breach event underscored the network's vulnerability to volumetric attacks and raised questions about the network's capacity to handle increased traffic [98].

With cutting-edge features like network slicing, eMBB, and the mMTC, the realm of potential cyber threats with 5G has expanded exponentially [30,66]. Within this landscape, network anomalies, characterized by unusual patterns or behaviors in network traffic, serve as harbingers of potential security threats, be it breaches, system vulnerabilities, or hardware malfunctions. With 5G set to power billions of IoT devices, ranging from smart home appliances to sophisticated industrial sensors, the sheer volume of data being relayed is staggering [68,70]. Detecting anomalous behavior within this data is critical, as it could indicate a device that has been compromised. A single compromised device, if overlooked, might serve as a backdoor to larger, more crucial systems, presenting significant security risks. Additionally, the introduction of network slicing in 5G, where various virtual networks operate on a shared physical infrastructure, further complicates the security

scenario. An undetected anomaly in one virtual network slice could potentially jeopardize the integrity of others. Furthermore, for applications that rely on 5G's URLLC, such as autonomous vehicles, real-time anomaly detection is a necessity for safety [99].

### 5. Current and Prospective Solutions to Enhance 5G Security

As we are witnessing an exponential growth in the deployment of 5G networks, it is imperative to address the associated security concerns [4]. These issues include technical vulnerabilities, regulatory ambiguities, and potential threats from a diverse group of malicious actors. To fortify the security stance of 5G networks, a myriad of current and prospective solutions is being explored. These solutions are multilayered and operate in various aspects of the network, such as technical, organizational, regulatory, and user-based levels. Technical solutions form the bedrock of 5G security, as they directly deal with the various threats and vulnerabilities [6]. The first line of defense usually involves robust encryption protocols. Advanced encryption standards, such as the 256-bit AES, are being used to secure communication channels in 5G networks. Moreover, ML and AI are increasingly playing a significant role in 5G network security. These technologies are used for anomaly detection, intrusion detection, and rapid response to potential threats [7]. They help in identifying patterns of malicious activities even when they vary from previously identified threats, thereby improving the network's adaptive capabilities. Blockchain technology is also being leveraged for decentralizing security control, which significantly reduces the chances of single-point security failure. blockchain technology can be utilized for secure device authentication in 5G networks [100]. Organizational and regulatory solutions are equally vital in enhancing 5G security. These involve the adoption of best practices, risk management frameworks, and adherence to international standards and regulations. Organizations are encouraged to adopt a risk-based approach for their cybersecurity initiatives. This involves identifying the most critical assets, potential threats to those assets, and implementing effective countermeasures. Regulatory bodies play a crucial role in ensuring adherence to the established security standards and guidelines. They work on the international harmonization of 5G security standards to avoid regional discrepancies and loopholes that may be exploited.

Traditional rule-based systems, designed for earlier network generations, find themselves outpaced by the dynamic and diverse nature of 5G traffic. Consequently, the arena of network security is witnessing a paradigm shift towards AI and ML security solutions [9,39]. These advanced technologies, with their capability to learn and adapt from data, are uniquely positioned to detect complex patterns and predict potential anomalies with impressive accuracy. By perpetually training on fresh data, they ensure that the detection mechanisms remain relevant to the ever-evolving threat environment.

Table 9 encapsulates various security solutions deployed in 5G networks, categorizing them based on their examples, strengths, and weaknesses. Machine learning and AI offer high adaptability and real-time threat detection but are resource-intensive. Blockchain technology provides robust IoT security but faces scalability issues. Software-Defined Networking and Network Function Virtualization contribute to enhanced network flexibility but introduce new vulnerabilities. Encryption methods like the AES and homomorphic encryption provide robust security but have their own limitations, such as speed and quantum resistance. Organizational measures help set security benchmarks but require initial investment and continuous compliance efforts. User education aims to reduce human-related errors but its effectiveness depends on continuous educational initiatives and user engagement [91,101,102].

As Table 9 articulates, there exists a broad landscape of security solutions pivotal to 5G infrastructures—ranging from machine learning and blockchain technology to encryption and authentication—Table 10 serves as a natural extension of this subsection, offering a detailed exploration of the complexities inherent in 5G encryption and authentication techniques. Specifically, Table 10 elaborates on the current methods, their key

features, strengths, weaknesses, and applicability, thereby complementing and enriching the foundational overview presented in Table 9.

**Table 9.** Security solutions in 5G [4,6,39,51,52].

Security Solutions in 5G	Examples	Strengths	Weaknesses
Machine learning (ML) and artificial intelligence (AI)	<ul style="list-style-type: none"> <li>- Intrusion detection using deep learning algorithms.</li> <li>- Pattern recognition for threat detection.</li> </ul>	<ul style="list-style-type: none"> <li>- High accuracy in identifying known and unknown threats.</li> <li>- Adaptability to evolving network patterns.</li> <li>- Real-time threat detection.</li> </ul>	<ul style="list-style-type: none"> <li>- Resource-intensive, potentially impacting network efficiency.</li> <li>- Need for continuous training and updates.</li> <li>- Susceptible to adversarial attacks.</li> </ul>
Blockchain technology	<ul style="list-style-type: none"> <li>- Secure device authentication in 5G IoT.</li> </ul>	<ul style="list-style-type: none"> <li>- Decentralization reduces single-point failure risks.</li> <li>- Robustness in IoT security.</li> <li>- Enhanced trust through transparency.</li> </ul>	<ul style="list-style-type: none"> <li>- Complex implementation and scalability challenges.</li> <li>- Slower transaction processing compared to centralized systems.</li> <li>- Energy-intensive consensus mechanisms.</li> </ul>
SDN and NFV	<ul style="list-style-type: none"> <li>- Adaptive network slicing.</li> <li>- Enhanced security through virtualization.</li> </ul>	<ul style="list-style-type: none"> <li>- Improved network agility and flexibility.</li> <li>- Enhanced protection against lateral movement threats.</li> <li>- Efficient resource utilization.</li> </ul>	<ul style="list-style-type: none"> <li>- Scalability and performance overhead concerns.</li> <li>- Complexity in managing virtualized network functions.</li> <li>- Potential vulnerabilities in virtualized environments.</li> </ul>
Encryption and authentication	<ul style="list-style-type: none"> <li>- Use of Advanced encryption standard (AES).</li> <li>- Homomorphic encryption for secure data processing.</li> <li>- Unified Authentication Framework (UAF).</li> <li>- Biometric authentication.</li> <li>- Blockchain-based authentication.</li> </ul>	<ul style="list-style-type: none"> <li>- AES offers a high level of security.</li> <li>- Homomorphic encryption allows secure data processing without decryption.</li> <li>- UAF provides flexibility in authentication methods.</li> <li>- Biometric authentication enhances identity verification.</li> <li>- Blockchain-based authentication decentralizes control.</li> </ul>	<ul style="list-style-type: none"> <li>- AES is not quantum-resistant.</li> <li>- Homomorphic encryption can be slow and complex.</li> <li>- Complexity and scalability challenges for UAF.</li> <li>- Biometric authentication may require specialized hardware.</li> <li>- Blockchain-based authentication can be complex to implement.</li> </ul>
Organizational and regulatory measures	<ul style="list-style-type: none"> <li>- Best practices adoption.</li> <li>- Risk management frameworks.</li> <li>- Compliance with international standards and regulations.</li> </ul>	<ul style="list-style-type: none"> <li>- Enhances overall security posture.</li> <li>- Provides benchmarks for security.</li> <li>- Fosters trust among stakeholders.</li> </ul>	<ul style="list-style-type: none"> <li>- Initial investment in security measures.</li> <li>- Compliance can be complex and time-consuming.</li> <li>- Varied regulations across regions.</li> </ul>
User education and awareness	<ul style="list-style-type: none"> <li>- Promoting digital literacy.</li> <li>- Raising cybersecurity awareness.</li> </ul>	<ul style="list-style-type: none"> <li>- Reduces human error-related security incidents.</li> <li>- Empowers users to protect themselves.</li> </ul>	<ul style="list-style-type: none"> <li>- Requires continuous educational efforts.</li> <li>- Users may remain susceptible to social engineering attacks.</li> <li>- Effectiveness depends on user willingness to engage.</li> </ul>

**Table 10.** Encryption and authentication techniques in 5G [17,48,49,60–63,76,100,103,104].

Encryption and Authentication Techniques in 5G	Current Techniques	Key Features	Strengths	Weaknesses	Applicability
Encryption techniques	<ul style="list-style-type: none"> <li>- Advanced encryption standard (AES): utilizes key lengths of 128, 192, and 256 bits.</li> <li>- Homomorphic encryption: enables secure computation on encrypted data.</li> </ul>	<ul style="list-style-type: none"> <li>- AES provides symmetric encryption for data confidentiality.</li> <li>- Homomorphic encryption allows privacy-preserving computation on encrypted data.</li> </ul>	<ul style="list-style-type: none"> <li>- AES offers strong security against known attacks.</li> <li>- Homomorphic encryption enhances data privacy in cloud and big data applications.</li> </ul>	<ul style="list-style-type: none"> <li>- AES is vulnerable to quantum computing attacks.</li> <li>- Homomorphic encryption introduces computational overhead.</li> </ul>	<ul style="list-style-type: none"> <li>- AES is widely used for data confidentiality in 5G communication.</li> <li>- Homomorphic encryption is suitable for privacy-preserving applications like cloud computing and data analysis.</li> </ul>

Table 10. Cont.

Encryption and Authentication Techniques in 5G	Current Techniques	Key Features	Strengths	Weaknesses	Applicability
Authentication techniques	<ul style="list-style-type: none"> <li>- UAF offers flexibility in authentication methods.</li> <li>- Biometric authentication: utilizes unique biological traits (e.g., fingerprints, facial recognition) for identity verification.</li> <li>- Blockchain-based authentication: decentralizes authentication, reducing the risk of single-point failures.</li> </ul>	<ul style="list-style-type: none"> <li>- UAF provides a unified framework for various authentication methods.</li> <li>- Biometric authentication relies on unique physical characteristics.</li> <li>- Blockchain-based authentication offers decentralized control and immutable records.</li> </ul>	<ul style="list-style-type: none"> <li>- UAF enhances security by allowing multiple authentication methods.</li> <li>- Biometric authentication provides strong identity verification.</li> <li>- Blockchain-based authentication increases resilience by decentralization.</li> </ul>	<ul style="list-style-type: none"> <li>- UAF may face complexity and scalability challenges in large-scale deployments.</li> <li>- Biometric authentication may require specialized hardware and raise privacy concerns.</li> <li>- Implementing blockchain-based authentication can be complex.</li> </ul>	<ul style="list-style-type: none"> <li>- UAF can be used for flexible authentication in diverse 5G network environments.</li> <li>- Biometric authentication is suitable for secure user identification in mobile and IoT devices.</li> <li>- Blockchain-based authentication enhances trust and security in 5G networks.</li> </ul>

*Analysis of Encryption and Authentication Techniques*

Encryption and authentication are foundational security measures for securing data transmission and ensuring that access to network resources is only granted to authorized users [61,76]. These measures are especially crucial in 5G networks due to their highly distributed nature and the sheer volume of data being transmitted, as shown in Table 10. Encryption techniques are essential for maintaining the confidentiality and integrity of data transmitted over 5G networks. In essence, encryption involves transforming the original data into an unreadable format that can only be reverted to its original form with the correct decryption key. The AES is widely used for data encryption in 5G networks. AES-256, in particular, offers a high level of security and is suited to protect sensitive data transmitted over these networks. Additionally, homomorphic encryption techniques are gaining attention due to their ability to perform computations on encrypted data, thus providing an extra layer of privacy in 5G applications like cloud computing and big data analysis [105,106]. Authentication techniques in 5G networks are designed to verify the identity of devices and users seeking access to the network, thereby preventing unauthorized access. One of the key enhancements in 5G networks over its predecessors is the introduction of the UAF [104]. The UAF allows for the flexibility to use various types of credentials and authentication methods, providing a more robust and flexible authentication mechanism. One of the emerging authentication methods is biometric authentication, which involves verifying an individual’s identity based on unique biological traits, such as fingerprints or facial recognition. Bedari et al. [107], demonstrated how biometric authentication can be efficiently used in 5G networks, they developed a secure, efficient online fingerprint authentication system for IIoT devices on 5G networks, featuring a novel cancelable fingerprint template to enhance data security and performance. Simultaneously, blockchain-based authentication techniques are also being explored for 5G networks. They offer a decentralized approach to authentication, reducing the risk of single-point failures [108].

Table 10 presents a detailed overview of the encryption and authentication techniques that are currently being employed in 5G networks. It categorizes these techniques based on their key features, strengths, weaknesses, and applicability. For encryption, the table contrasts the AES with homomorphic encryption. The AES offers robust symmetric encryption, securing data confidentiality effectively against most known attacks. However, its primary drawback lies in its vulnerability to quantum computing attacks. In contrast, homomorphic encryption allows for privacy-preserving computations on encrypted data, making it particularly beneficial for cloud and big data applications. Yet, it introduces computational overhead, which may be a limitation in resource-constrained settings. On the authentication side, the UAF offers flexibility by accommodating various authentication methods, enhancing security. However, its complexity and scalability could be challenging for large-scale deployments. Biometric authentication, leveraging unique biological traits like fingerprints, offers strong identity verification but may require specialized hardware and elicit privacy concerns. Blockchain-based authentication decentralizes control, thus in-

creasing resilience against single-point failures, but its implementation complexity remains an obstacle.

## 6. Machine Learning and 5G Security

This section discusses the role of ML in enhancing 5G security and the solutions that it provides, further we discuss the ML applications in 5G security, optimize the functioning of security protocols in 5G networks and how to optimize the functioning of security protocols in 5G networks. However, emerging security measurements like attribute-based access controls and block chain-based access controls can take advantage of ML to strengthen their advancement in 5G security.

### 6.1. The Role of Machine Learning in Enhancing 5G Security

The use of ML algorithms offers an advanced and effective solution to enhance and reduce the security challenges associated with the advent of 5G networks [7,8]. The inherent attributes of ML, such as adaptability, prediction capability, and large-scale data processing, provide promising solutions to handle the unprecedented scale and complexity of the 5G ecosystem. The onset of 5G networks has brought about a paradigm shift in the world of telecommunications, promising high-speed connectivity, low latency, and a seamless integration of billions of devices across the globe. However, this immense progress also brings with it a range of novel security challenges that require innovative solutions. ML algorithms can help to develop intelligent 5G security systems capable of self-learning and adapting to evolving threats, allowing for real-time threat detection and mitigation [7,39]. Furthermore, ML algorithms are capable of processing massive volumes of data generated by 5G networks, extracting valuable insights about possible threats and providing proactive security measures to prevent potential attacks [109]. ML has emerged as a potent tool in this context, offering robust capabilities to improve the security framework in 5G networks. Machine learning, with its capabilities for pattern recognition, anomaly detection, and predictive modeling, plays a pivotal role in strengthening the security apparatus of 5G networks [39,109].

The implementation of ML in 5G security is thereby poised to significantly improve the robustness and reliability of the 5G infrastructure, contributing to the overall sustainability of the digital ecosystem in the era of 5G and beyond. Generally, the role of ML in 5G security is multifaceted, spanning areas like intrusion detection, privacy preservation, secure routing, and threat intelligence, among others. It holds the potential to transform the conventional, reactive security frameworks into proactive, intelligent systems capable of thwarting cyberattacks before they can inflict significant damage [110].

The potential of ML in the realm of 5G security enhancement is significant. As 5G networks evolve into dynamic and complex systems, traditional security measures struggle to effectively manage the extensive network topology, heterogeneous traffic patterns, and multi-dimensional data. Machine learning is particularly adept at handling these challenges, as its capabilities extend beyond mere rule-based systems. In 5G networks, ML algorithms can intelligently process vast amounts of network data, promptly recognizing potential security threats through anomaly detection [111]. The capability of ML to learn from past data and experiences allows it to accurately distinguish normal network behavior from malicious activities, providing effective real-time threat detection. Moreover, through predictive analytics, ML can foresee potential attacks, giving network operators valuable lead time to mitigate potential damages. Another key strength of ML is its adaptability, which enables it to learn from new situations and update its predictive models accordingly. This continuous learning feature is vital for coping with the evolving nature of cyber threats in 5G networks. Moreover, ML can improve resource allocation and optimize security protocols, enhancing both network security and performance [112].

A myriad of machine learning techniques holds substantial relevance in the realm of 5G security, offering unique capabilities for different aspects of network security management [113]. Supervised learning techniques such as support vector machines (SVMs)



and decision trees are commonly used for intrusion detection in 5G networks [114]. These algorithms learn from labeled training data to classify network activities as either normal or malicious [115]. In particular, decision trees are beneficial for their ease of interpretation, enabling network administrators to understand the decision-making process behind the detection of potential threats. Unsupervised learning algorithms like k-means clustering, Linear Regression, supervised classifier and hierarchical clustering are valuable for anomaly detection, identifying unusual patterns in network data that may signify a security breach [116,117]. These algorithms do not require labeled data, making them flexible tools for discovering unknown threats. Reinforcement learning, a type of ML where an agent learns to make decisions by interacting with its environment, has shown promise in the area of network intrusion response. By iteratively adjusting its actions based on received rewards or punishments, a reinforcement learning agent can determine the optimal actions to mitigate detected intrusions [118].

Table 11 reports the role of various machine learning techniques in enhancing the security in 5G networks, showing the advantages and limitations of each technique along with the metrics commonly employed for evaluation. Supervised learning is prominently used in applications like IDS and spam filtering. Its high accuracy in identifying known threats and low false-positive rates are notable strengths. However, the technique does necessitate labeled data and is susceptible to overfitting. Typical evaluation metrics include accuracy and the precision–recall curve. Unsupervised learning finds utility in anomaly detection and network traffic clustering. It eliminates the need for labeled data and can unearth previously unidentified threats. Despite these merits, it has lower accuracy compared to supervised learning techniques and incurs high computational costs. Metrics like cluster purity and silhouette score are commonly used for evaluation. Reinforcement learning facilitates adaptive network configurations and policy-based security measures. Its ability to learn optimal policies over time and adapt to evolving network conditions is laudable. However, extensive training data are required, and the complexity of defining appropriate reward functions is a challenge. Cumulative reward and convergence time are key metrics for evaluation. Ensemble methods, often used to enhance IDS capabilities and combine multiple classifiers, are praised for their improved generalization and resistance to overfitting. However, they are computationally demanding and can be complex to interpret. Evaluation is typically conducted using cross-validation scores and the F1 score. Lastly, neural networks, which are used for deep packet inspection and malware identification, are robust in feature representation and excel at capturing complex patterns. These strengths are offset by their resource-intensive nature and risk of overfitting, especially with small datasets. Area Under the Receiver Operating Characteristic (AUROC) and F1 score are standard evaluation metrics.

**Table 11.** Machine learning security existing solutions in 5G [7,39,109,110,112,113,115,118,119].

ML Techniques in 5G Security	Applications	Strengths	Weaknesses	Evaluation Metrics
Supervised learning	- IDS - Spam filtering	- High accuracy in known threat detection - Low false-positive rates	- Requires labeled data for training - Susceptible to overfitting	- Accuracy - Precision–recall curve
Unsupervised learning	- Anomaly detection - Network traffic clustering	- No need for labeled data - Can identify previously unseen threats	- Lower accuracy compared to supervised methods - High computational cost	- Cluster purity - Silhouette score
Reinforcement learning	- Adaptive network configuration - Policy-based security measures	- Capable of learning optimal policies over time - Adapts to changing network conditions	- Requires extensive training data - Complexity in setting reward functions	- Cumulative reward - Convergence time
Ensemble methods	- Boosting IDS capabilities - Combining multiple classifiers	- Improved generalization - Resistance to overfitting	- Computationally expensive - Complexity in interpretation	- Cross-validation score - F1 score

Table 11. Cont.

ML Techniques in 5G Security	Applications	Strengths	Weaknesses	Evaluation Metrics
Neural networks	- Deep packet inspection - Malware identification	- High capability for feature representation - Good at capturing complex patterns	- Resource-intensive - Risk of overfitting in small datasets	- Area Under the Receiver Operating Characteristic (AUROC) - F1 score

### 6.2. Machine Learning Applications in 5G Security

Machine learning, with its advanced analytical capabilities, is instrumental in various applications within 5G security [120,121]. These applications span across diverse domains such as intrusion detection, malware mitigation, and predictive security modeling. In the context of intrusion detection, machine learning algorithms analyze network traffic data to identify patterns that deviate from the norm. SVM and decision trees, for instance, have demonstrated effectiveness in classifying network activities and detecting potential intrusions [122,123]. Such techniques greatly enhance the security system's responsiveness and accuracy, thereby minimizing the risk of successful cyberattacks. Machine learning is also pivotal in combating malware. It facilitates the identification and classification of harmful software based on their behavioral characteristics and binary features. For instance, deep learning methods such as CNNs are highly efficient in extracting and learning complex features from large-scale data, allowing for effective detection of zero-day malware [124]. Predictive security modeling is another area where machine learning holds significant potential. Leveraging algorithms such as logistic regression and random forests, predictive models can forecast potential vulnerabilities and threats based on historical data and ongoing network activities. This enables proactive defense measures, thereby improving the resilience of 5G networks against sophisticated cyber threats [124].

#### 6.2.1. Anomaly Detection

Anomaly detection is a paramount task in maintaining the security of 5G networks. This involves the identification of unusual patterns or deviations from the expected behavior, which could indicate potential threats or network malfunctions. Several machine learning techniques have been employed in anomaly detection tasks. For instance, clustering algorithms like k-means can group network traffic data based on similar characteristics, allowing for the detection of outliers or anomalies [125]. Classification algorithms, on the other hand, can be trained to distinguish between normal and anomalous network behaviors. In particular, SVMs and decision trees have shown effectiveness in this regard. Moreover, advancements in machine learning have brought forth more sophisticated techniques such as deep learning, which are capable of detecting more complex and subtle anomalies. Techniques such as autoencoders, a type of artificial neural network, are able to learn a compressed representation of the input data and then reconstruct the original data. When trained on normal data, the model would generate high reconstruction errors for anomalous data, thereby identifying the anomalies [125]. These machine learning-driven anomaly detection techniques not only enhance the accuracy of detection but also reduce the time taken to detect and mitigate potential security threats, significantly boosting the resilience of 5G networks.

#### 6.2.2. Security Predictions Using Machine Learning

Predictive security is a proactive approach in cybersecurity where ML can play an integral role in different areas, particularly in 5G networks. Security predictions using ML involve forecasting future security incidents by leveraging historical and real-time network data. This ability to foresee potential threats offers a strategic advantage, allowing the network to take proactive measures to minimize or prevent harm. A variety of machine learning techniques are applicable to this task, including classification, regression, and time-series forecasting. For instance, logistic regression, random forest, and gradient boosting can be utilized for predicting security incidents based on historical data patterns [109,126].

Furthermore, Long Short-Term Memory (LSTM) networks, a type of RNN specialized in processing sequences of data, have been effectively used in time-series forecasting for predictive security. They can model the temporal dependencies in network traffic data, thereby predicting future anomalies or intrusions. One prominent application of ML for security predictions in 5G is the anticipation of DDoS attacks. Through analyzing patterns in network traffic, ML algorithms can predict an impending DDoS attack and implement preventive measures, thus averting network downtime and potential loss of service. However, while ML holds considerable promise for predictive security, it is crucial to note that prediction models must continually evolve in response to the dynamic nature of 5G networks and the ever-changing landscape of cyber threats [8]. The role of machine learning in 5G security is shown in Table 11.

6.3. Security Protocol Optimization with Machine Learning

ML can also be leveraged to optimize the functioning of security protocols in 5G networks. The objective of security protocol optimization is to enhance the network’s security performance without excessively consuming computational resources or impacting the network’s operational efficiency [127]. One critical area where ML can be utilized is in the optimization of key management protocols, a cornerstone of secure communications in 5G networks. ML algorithms can learn and predict the optimal times for key rotations, thereby increasing the security of encrypted communications while minimizing the overhead associated with the frequent key changes [128]. In addition, machine learning can be used to optimize IDS. Traditional IDS suffer from high false-positive rates, inefficient use of resources, and lack of adaptability. With ML, these systems can be optimized by enhancing their accuracy, improving resource allocation, and enabling them to adapt to evolving threat landscapes. ML can also aid in the optimization of security configurations and policies. Given the complexity of 5G networks, managing and optimizing security settings can be a daunting task. ML algorithms can learn from past incidents, analyze the impact of various configurations, and suggest optimal settings to enhance the security posture of the network [129]. However, it should be noted that the use of ML for security protocol optimization is not without challenges. The effectiveness of ML techniques hinges on the quality and comprehensiveness of the available data. Moreover, the complexity of ML models can sometimes lead to a lack of interpretability, which may pose challenges in understanding and validating the optimized protocols [95].

Table 12 illustrates a comprehensive framework for understanding the role and utility of ML techniques in fortifying 5G network security. The table is structured across multiple dimensions, elaborating on the applications, key techniques, advantages, and challenges of implementing ML in a 5G context. It spans various aspects, from real-time threat detection to predictive security modeling and anomaly identification, encompassing both supervised and unsupervised learning paradigms. The advantages frequently cited include real-time threat mitigation, enhanced network security, and the adaptability to evolving cyber threats. Despite the compelling benefits, the table also highlights key challenges, including data privacy concerns, computational overhead, and issues related to scalability and data quality.

Table 12. Machine learning in 5G security [105,108,111,130–144].

Machine Learning in 5G Security	Applications	Key Techniques	Advantages	Challenges
Role of ML in 5G security	<ul style="list-style-type: none"> <li>- Real-time threat detection and mitigation</li> <li>- Proactive security measures</li> <li>- Large-scale data processing</li> </ul>	<ul style="list-style-type: none"> <li>- Pattern recognition</li> <li>- Anomaly detection</li> <li>- Predictive modeling</li> </ul>	<ul style="list-style-type: none"> <li>- Real-time threat detection</li> <li>- Improved security posture</li> <li>- Adaptation to evolving threats</li> </ul>	<ul style="list-style-type: none"> <li>- Data privacy concerns</li> <li>- Complexity of implementation</li> </ul>

Table 12. Cont.

Machine Learning in 5G Security	Applications	Key Techniques	Advantages	Challenges
Potential of ML in security enhancement	<ul style="list-style-type: none"> <li>- Intrusion detection</li> <li>- Anomaly detection</li> <li>- Predictive security modeling</li> <li>- Adaptive security mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>- Supervised learning (e.g., SVM, decision trees)</li> <li>- Unsupervised learning (e.g., clustering)</li> <li>- Reinforcement learning</li> </ul>	<ul style="list-style-type: none"> <li>- Enhanced network security</li> <li>- Efficient threat detection</li> <li>- Adaptive security mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>- Data quality and labeling issues</li> <li>- Resource-intensive</li> </ul>
Pertinent ML techniques in 5G security	<ul style="list-style-type: none"> <li>- Intrusion detection</li> <li>- Anomaly detection</li> <li>- Network intrusion response</li> <li>- Adaptive security</li> </ul>	<ul style="list-style-type: none"> <li>- Supervised learning (e.g., SVM, decision trees)</li> <li>- Unsupervised learning (e.g., clustering)</li> <li>- Reinforcement learning</li> </ul>	<ul style="list-style-type: none"> <li>- Effective intrusion detection</li> <li>- Anomaly detection</li> <li>- Adaptive response</li> </ul>	<ul style="list-style-type: none"> <li>- Training data availability</li> <li>- Scalability for large networks</li> </ul>
Applications of ML in 5G security	<ul style="list-style-type: none"> <li>- Intrusion detection</li> <li>- Malware mitigation</li> <li>- Predictive security modeling</li> <li>- Anomaly detection</li> <li>- Predicting DDoS attacks</li> </ul>	<ul style="list-style-type: none"> <li>- Classification</li> <li>- Regression</li> <li>- Time-series forecasting</li> <li>- Deep learning (e.g., LSTM)</li> </ul>	<ul style="list-style-type: none"> <li>- Early threat detection</li> <li>- Improved network resilience</li> </ul>	<ul style="list-style-type: none"> <li>- Model overfitting</li> <li>- False positives/negatives</li> </ul>
Anomaly detection through ML	<ul style="list-style-type: none"> <li>- Identification of unusual patterns</li> <li>- Detection of security threats</li> <li>- Reduced detection time</li> </ul>	<ul style="list-style-type: none"> <li>- Clustering (e.g., k-means)</li> <li>- Classification (e.g., SVM, decision trees)</li> <li>- Deep learning (e.g., autoencoders)</li> </ul>	<ul style="list-style-type: none"> <li>- Precise anomaly detection</li> <li>- Reduced false alarms</li> </ul>	<ul style="list-style-type: none"> <li>- Complex model tuning</li> <li>- Scalability for high-speed networks</li> </ul>
Security predictions using ML	<ul style="list-style-type: none"> <li>- Predicting security incidents</li> <li>- Anticipating DDoS attacks</li> <li>- Proactive defense measures</li> </ul>	<ul style="list-style-type: none"> <li>- Classification (e.g., logistic regression, random forest)</li> <li>- Time-series forecasting (e.g., LSTM)</li> </ul>	<ul style="list-style-type: none"> <li>- Early threat anticipation</li> <li>- Proactive security measures</li> </ul>	<ul style="list-style-type: none"> <li>- Model drift over time</li> <li>- Data labeling challenges</li> </ul>

Further, the supervised and unsupervised learning classification for 5G researchers is summarized in Table 13.

Table 13. Supervised and unsupervised learning classification for 5G researchers.

Learning Problem	ML Algorithm	Study Example
Supervised learning	Linear Regression	Moore, J.H.; Lamb, J.M.; Brown, N.J.; Vaughan, D.E. (2002) [116]
	Supervised Classifier	Peng, C.; Fan, W.; Huang, W.; Zhu, D. (2023) [117]
	SVM	Anand, A., Rani, S., Anand, D., Aljahdali, H. M., Kerr, D. (2021) [114]
	Neural network	Kimura, B. Y. L., Almeida, J. (2021) [145]
	Artificial neural networks (ANNs)	Santos, G. L., Endo, P. T., Sadok, D., Kelner, J. (2020) [146]
Unsupervised learning	Deep neural networks (DNNs)	Ali, S., Haider, A., Rahman, M., Sohail, M., Zikria, Y. B. (2021) [101]
	k-means clustering	Kodinariya, T. M., Makwana, P. R. (2013) [91]
	Hierarchical clustering	Lin, C.C.; Tsai, C.T.; Liu, Y.L.; Chang, T.T.; Chang, Y.S. (2023) [102]
	Unsupervised soft clustering	Gupta, A.; Ghanshala, K.; Joshi, R.C. (2021) [147]
	Self-organizing map (SOM)	Li, J., Zhao, Z., Li, R. (2018) [148]
	Autoencoders (AEs)	Lam, J.; Abbas, R. (2020) [119]
	Adversarial autoencoders	Sevgican, S., Turan, M., Gökarslan, K., Yilmaz, H. B., Tugcu, T. (2020) [149]
Generative deep neural networks (GDNNs)	Ferreira, D., Reis, A. B., Senna, C., Sargento, S. (2021) [130]	
Affinity Propagation Clustering	Radivilova, T., Kirichenko, L., Lemeshko, O., Ageyev, D., Mulesa, O., Ilkov, A. (2021, September) [131] Boukerche, A., Zhang, Q. (2019) [108]	

Table 13 provides an in-depth taxonomy of both supervised and unsupervised learning algorithms that have been employed in the realm of 5G research, according to prominent scholarly publications. The table is particularly useful for academic researchers focusing on machine learning applications in 5G networks. In the domain of supervised learning, the table catalogs a variety of algorithms from Linear Regression to DNNs. Each entry is accompanied by authoritative citations, thus serving as both a summary and a guide for further reading. For example, Gupta et al. [147] have contributed to Linear Regression,

while Ali et al. [101] have worked on the intricacies of deep neural networks within a 5G context. The unsupervised learning section of the table is similarly exhaustive, covering methodologies ranging from k-means clustering to Affinity Propagation Clustering.

## 7. Overview of Deep Learning in 5G Security

Deep learning is a subset of machine learning that leverages multiple layers of non-linear processing units for feature extraction and transformation, learning multiple levels of representation from raw input data [9,124]. These models are generally based on artificial neural networks, particularly CNNs and RNNs, and are designed to automatically and adaptively learn the spatial hierarchies of features. Within the realm of 5G security, deep learning brings about transformative potential with its capacity to analyze large datasets and recognize complex behavior and hidden patterns. DL algorithms are highly capable of detecting irregularities that could signal potential threats [101,145,146]. These abilities extend beyond mere detection, with algorithms capable of implementing defense mechanisms within milliseconds, a speed that is becoming increasingly critical in the hyper-connected 5G landscape. In addition to its superior processing abilities, DL also boasts self-learning capabilities, which are particularly beneficial for 5G networks that continuously generate a huge amount of data [132]. With traditional machine learning, the feature extraction process requires manual intervention, whereas deep learning models can learn these features directly from data, saving significant time and resources while also enhancing the accuracy of threat detection and response [124,133]. However, despite the enormous potential that DL holds for 5G security, it is not without its challenges. These include computational intensity, difficulties in understanding how DL makes its decisions (i.e., black box problem), and the risk of adversarial attacks. In addition, Abidi, M. H., Alkhalefah, H [150] investigated the role of ML and DL algorithms in optimizing network data analytics for 5G cellular networks. Given the rise in connected devices and associated data, traditional analytics methods are proving insufficient. The authors highlighted the challenges faced, such as handling vast amounts of data and privacy concerns. They emphasized the efficacy of ML and DL in recognizing data patterns, which aids in real-time decisions, proactive management, and enhanced 5G network reliability. Mu, J. [106] examined mobile crowd sensing (MCS) systems that rely on public participation through their mobile devices for data collection. The central challenge is incentivizing participation. The authors introduced "INCEPTION", a unique MCS framework that integrates incentives with data aggregation and perturbation, ensuring both data accuracy and privacy. This integrated approach was validated through both theoretical and simulation-based methods.

The evolution towards the 5G networks has significantly altered the telecommunication landscape, introducing unprecedented connectivity speed, massive network capacity, and reduced latency. However, the substantial benefits of 5G technology come with intricate security concerns primarily due to the massive scale, heterogeneity, and complexity of these networks. Therefore, it becomes imperative to leverage advanced, intelligent analytical tools that can adapt and respond to the ever-evolving security landscape. One such technology is DL, which has shown immense promise in cyber security applications. Deep learning, a subfield of machine learning, models high-level abstractions in data through the use of multiple layers of artificial neural networks [134]. What sets it apart from traditional machine learning is its ability to automatically learn representations from input data, eliminating the need for manual feature extraction. This self-learning capability is highly beneficial in a 5G context where networks continuously generate vast amounts of data. The capability to extract meaningful features from this sea of data allows DL algorithms to identify and react to complex patterns indicative of cyber threats [135]. More specifically, deep learning's superiority lies in its ability to teach computers to process data in a manner analogous to the human brain's processing. This characteristic, known as end-to-end learning, allows deep learning models to automatically learn hierarchical feature representations from raw input data, such as network traffic in a 5G environment, leading to more accurate predictions and threat detections. Moreover, given the dynamism and



volatility of 5G networks, the adaptive and robust nature of deep learning becomes even more critical. Through deep neural networks, DL models can adapt to new information, ‘learn’ from it, and ‘improve’ their threat detection and response strategies. Consequently, they provide a proactive approach to security, which is a crucial requirement for securing complex, rapidly evolving 5G networks [136].

### *7.1. Importance and Role of Deep Learning*

In the context of 5G security, the importance and role of DL cannot be overstated. One of the significant challenges faced by 5G networks is the vast amount of data being transmitted and received, which calls for advanced, efficient, and intelligent security solutions. With its ability to model high-level abstractions in data through the use of multiple processing layers, deep learning has emerged as a powerful tool for handling the intricacies of 5G security [137]. Primarily, deep learning excels in identifying, classifying, and mitigating potential security threats in 5G networks. Fifth-generation networks consist of numerous interconnected nodes, each producing and receiving a significant amount of multi-dimensional data. This data complexity and volume can be overwhelming for traditional security methods, resulting in missed or false alarms [138]. Deep learning, however, can analyze these data with a high degree of accuracy, using its complex, multi-layered neural networks to identify subtle patterns and anomalies that may be indicative of an impending attack or an ongoing security breach [111]. Moreover, deep learning has a self-learning or adaptive learning capability that sets it apart from traditional machine learning methods. This capability allows deep learning models to ‘learn’ from new information, continuously updating their knowledge and improving their performance over time. In the context of 5G security, this means that the network’s defense mechanism can continually enhance itself, becoming more effective and efficient at identifying and responding to emerging threats [139]. This proactive and adaptive approach to security is particularly vital given the rapid evolution of cyber threats and the increasing complexity of 5G networks.

### *7.2. Relevant Deep Learning Techniques for 5G Security*

As the demands of 5G security continue to grow, researchers have explored a variety of deep learning techniques to create robust and efficient security solutions. Among these, CNNs, RNNs, and Deep Belief Networks (DBNs) have emerged as particularly effective methods for enhancing 5G security [140].

CNNs are a type of deep learning model that are particularly well-suited for processing grid-like data, such as images and time-series data. In the context of 5G security, CNNs can be used to analyze the network traffic, identifying complex patterns and anomalies that may be indicative of security threats [141]. For instance, a CNN could analyze the traffic flow between different network nodes, identifying suspicious or irregular activities that might signal a potential cyberattack. Moreover, the convolutional layers in CNNs are efficient in detecting local patterns within the data, which can be instrumental in identifying localized attacks in the network [142].

RNNs are another deep learning model that are uniquely equipped to handle sequential data by retaining information from previous inputs in their hidden layers. This makes them particularly relevant for 5G security, as they can be used to analyze sequential or time-series data such as network logs or packet flows, identifying patterns and anomalies over time that may suggest an ongoing or imminent security breach [143]. Furthermore, the recurrent nature of RNNs allows them to remember past events, which is essential for detecting slow, progressive attacks that unfold over a period of time.

Table 14 provides a detailed overview of the role of deep learning techniques in the realm of 5G security, offering insights into the applications, strengths, and weaknesses of various approaches. From convolutional networks adept at image analysis to recurrent networks designed for sequence-based tasks, each method comes with its own set of advantages and limitations. While some excel in handling specific types of data or offer

advantages in scalability, they may require significant computational resources or face challenges such as overfitting and model complexity.

**Table 14.** Deep learning security solutions in 5G [132–141].

Deep Learning Techniques in 5G Security	Applications	Strengths	Weaknesses
Convolutional neural networks (CNNs)	<ul style="list-style-type: none"> <li>- Image-based authentication</li> <li>- Traffic pattern recognition</li> </ul>	<ul style="list-style-type: none"> <li>- Efficient in spatial data analysis</li> <li>- Robust to image transformations</li> </ul>	<ul style="list-style-type: none"> <li>- Requires large labeled datasets</li> <li>- Computationally intensive</li> </ul>
Recurrent neural networks (RNNs)	<ul style="list-style-type: none"> <li>- Sequence-based anomaly detection</li> <li>- Time-series analysis in network traffic</li> </ul>	<ul style="list-style-type: none"> <li>- Effective for sequential data</li> <li>- Capable of modeling long-term dependencies</li> </ul>	<ul style="list-style-type: none"> <li>- Difficult to train</li> <li>- Susceptible to vanishing and exploding gradient problems</li> </ul>
Generative adversarial networks (GANs)	<ul style="list-style-type: none"> <li>- Data augmentation for intrusion detection</li> <li>- Anomaly detection</li> </ul>	<ul style="list-style-type: none"> <li>- Ability to generate new data samples</li> <li>- Effective for semi-supervised learning</li> </ul>	<ul style="list-style-type: none"> <li>- Requires balanced dataset for effective training</li> <li>- Complexity in model convergence</li> </ul>
Autoencoders	<ul style="list-style-type: none"> <li>- Anomaly detection</li> <li>- Feature reduction for other ML models</li> </ul>	<ul style="list-style-type: none"> <li>- Effective for dimensionality reduction</li> <li>- Capable of learning data representations</li> </ul>	<ul style="list-style-type: none"> <li>- Risk of overfitting</li> <li>- Sensitivity to hyperparameters</li> </ul>
Transformer networks	<ul style="list-style-type: none"> <li>- Natural Language Processing for cybersecurity (e.g., phishing detection)</li> <li>- Complex event processing</li> </ul>	<ul style="list-style-type: none"> <li>- Capable of capturing long-range dependencies</li> <li>- Scalable and parallelizable architecture</li> </ul>	<ul style="list-style-type: none"> <li>- Requires substantial computing resources</li> <li>- May need large datasets for effective training</li> </ul>

### 7.3. Deep Learning Applications in 5G Security

The practical applications of deep learning in the context of 5G security are vast and diverse. As 5G networks increase in complexity and scale, the role of advanced techniques such as deep learning in ensuring network security becomes increasingly pivotal. Various deep learning models have been successfully applied to areas such as anomaly detection, threat prediction, and even intrusion detection systems in 5G networks [106].

**Anomaly detection:** One of the main applications of deep learning in 5G security is anomaly detection. Anomaly detection in network traffic refers to identifying patterns that do not conform to expected behavior, which could be indicative of a potential security threat or attack. Deep learning algorithms, especially unsupervised learning models like autoencoders, have proven effective in detecting anomalies in high-dimensional data. They can model the ‘normal’ behavior of the network and can effectively identify deviations or anomalies from this established norm.

**Threat prediction:** Deep learning can also be used for threat prediction in 5G networks. By analyzing historical network data, deep learning algorithms can identify patterns and trends that might suggest a future attack. RNNs, in particular, are very effective at this task due to their ability to process sequential data and remember past inputs, which is critical for understanding time-dependent patterns and trends in network data [95].

**IDSs:** Deep learning-based IDSs are another important application in 5G security. IDSs can monitor network traffic for suspicious activity or violations of policy. A deep learning-based IDS can learn and evolve with the ever-changing threat landscape, thereby improving its detection capabilities over time. Furthermore, deep learning algorithms can classify different types of attacks, thus enabling the system to respond appropriately to the specific threat at hand [140].

#### 7.3.1. Improving Intrusion Detection Systems

IDSs are a fundamental component of network security, serving as a first line of defense against potential security breaches. They function by identifying unusual or suspicious activity in network traffic that could indicate an attempted intrusion [144]. However, traditional IDSs often rely on predefined rules and signatures to detect intrusions, which

may not be effective against novel or sophisticated attacks. This is where deep learning can make a significant contribution to improving the efficacy of IDSs in 5G networks. By applying deep learning models, IDSs can be trained to identify both known and unknown threats in real time. For instance, deep learning techniques such as CNNs have been used to develop IDSs that can learn to recognize intrusion attempts based on patterns in network traffic [140]. Similarly, RNNs, which can process sequential data, can identify temporal patterns in network traffic that may indicate an ongoing or imminent attack.

Another way deep learning can enhance IDSs is by reducing the number of false positives, which are the incorrect identification of normal activities as intrusions. High rates of false positives can overwhelm network administrators and potentially result in genuine threats being overlooked. Deep learning algorithms can learn the normal behavioral patterns of a network over time and become more accurate in distinguishing between actual intrusions and benign network activity, thereby reducing false positives [151].

### 7.3.2. Mitigating Malware Risks Using Deep Learning

As the complexity and sophistication of cyber threats grow, particularly in the context of 5G technology, the risks posed by malware—malicious software designed to cause harm to a system or network—become increasingly significant. Malware can take many forms, including viruses, worms, trojans, ransomware, and spyware, and the detection and prevention of such threats is a key aspect of maintaining 5G network security [128]. Deep learning techniques have shown remarkable potential in mitigating malware risks in 5G networks. These techniques can go beyond traditional, signature-based malware detection methods, which are often ineffective against zero-day and polymorphic malware, by learning to recognize malicious patterns and behaviors in software applications or network traffic [129]. For instance, deep learning models like RNNs and LSTM can analyze sequences of system calls made by applications, enabling the detection of previously unseen or unknown malware based on their behavioral patterns. Furthermore, CNNs, known for their prowess in image recognition tasks, have been applied successfully to malware detection, treating binary files as images and identifying harmful patterns therein. Additionally, autoencoders, a specific type of artificial neural network, have been utilized in unsupervised learning scenarios for malware detection. They can learn the normal behavior of a system and identify any deviations which could signify a malware infection [95].

### 7.3.3. Deep Learning Models for Security Prediction

One of the foremost challenges in maintaining the security of 5G networks lies in the ability to anticipate and respond to potential threats before they can cause significant harm. This requires the development of predictive models that can analyze past and present network data to identify potential future security issues. Deep learning, with its inherent capabilities in handling vast volumes of complex data, provides an efficient means to build such predictive models. Deep learning algorithms like LSTM and GRU, both variations of RNNs, have demonstrated significant promise in this context [127]. By virtue of their design, these algorithms can process temporal sequences of data characteristics, which is especially valuable when dealing with network data that evolve over time. By training these deep learning models on historical network data, including instances of past security breaches, it is possible to create a predictive model that can foresee potential security risks. These predictive models can detect early signs of unusual network behavior, helping security teams to address threats before they escalate into major security incidents proactively. For instance, LSTM and GRU can be trained to detect patterns indicative of DDoS attacks, one of the most common and damaging forms of cyberattack [151]. By identifying these patterns early, it is possible to take preventive measures and minimize the potential harm to the 5G network.

## 8. Technical and Ethical Considerations for Effective Implementation of 5G Security

### 8.1. Technical Considerations

The primary technical considerations for effective implementation of 5G security involve architectural modifications, cryptographic techniques, and adaptive security protocols. The 5G network architecture is fundamentally different from previous generations, enabling more devices and facilitating data-driven applications. However, this complexity increases the vulnerable surface area. Robust cryptographic techniques are thus essential to ensure data integrity, confidentiality, and secure user authentication. Further, the dynamism of 5G networks necessitates adaptive security protocols that can adjust to varying levels of threats and vulnerabilities. Machine learning and deep learning technologies, as delineated in previous sections, offer promising avenues to bolster adaptive security mechanisms but bring their own set of challenges like training data quality, model interpretability, and computational cost.

### 8.2. Ethical Considerations

Ethically, the implementation of 5G security faces multifaceted challenges. Data privacy stands as a paramount concern; ensuring that the advanced data collection capabilities of 5G networks do not compromise user privacy is critical. Algorithmic decision making, pivotal in machine learning-based security solutions, must be transparent and accountable to avoid issues like false positives in intrusion detection or algorithmic bias. Additionally, access to secure and robust 5G technology needs to be equitable to prevent economic and social stratification. This ethical mandate extends to environmental considerations, where the rapid obsolescence and replacement of hardware components should be managed responsibly to minimize electronic waste and environmental impact.

### 8.3. Integrated Approach for Effective Implementation

For the effective implementation of 5G security, both technical and ethical considerations need to be integrated cohesively into a holistic framework. Technological solutions should be designed and deployed with ethical guidelines in mind, ensuring that advancements in security do not come at the cost of privacy or equity. Likewise, ethical considerations should be technically feasible and not hamper the performance or effectiveness of the security solutions. Standardization bodies and governance organizations have a significant role to play in ensuring that technical specifications include ethical mandates. Moreover, a multidisciplinary approach involving technologists, ethicists, policymakers, and legal experts is essential for comprehensively addressing the intricate landscape of 5G security.

## 9. Conclusions and Future Work

The advent of the 5G network paved the way for innovative applications across various sectors, promising unparalleled data speeds, lower latency, and increased connectivity. However, the complex architecture and broader attack surface of 5G networks introduce profound security threats that necessitate meticulous analysis and robust countermeasures. This research embarks on a comprehensive journey through the nuanced domain of 5G mobile network security, accentuating the transformative role of machine learning (ML) and deep learning (DL). This study offers a multifaceted analysis, providing an exhaustive exposition of the current security architectures, inherent challenges, and integral functionalities specific to 5G networks. Secondly, it delves into a meticulous assessment of distinct vulnerabilities and robust features, particularly emphasizing network slicing and mMTC. In doing so, it identifies and elaborates on specific security threats that are either novel or amplified within the 5G context, enriching the existing threat framework. This research transitions into a problem-solving phase by investigating ML and DL's efficacy and potential in bolstering 5G security, highlighting their practical applications in critical areas, including anomaly detection, predictive security, and malware risk mitigation. Finally, this work is a seminal reference that guides future innovations and strategic advancements in 5G security.

### Guidance for Future Research

Our study points to crucial areas for future research, emphasizing the need to investigate further machine learning and deep learning algorithms specific to 5G's dynamic settings. Future work should aim to develop comprehensive security protocols that integrate robust architecture with advanced computation. Additionally, exploring user behavior after security breaches could provide valuable insights for creating more user-focused, resilient security solutions in future 5G networks. More exploration into distributed ML, federated learning, and privacy-preserving continual learning is expected to lead the domain.

**Author Contributions:** H.N.F., S.A. and M.A. were instrumental in the conceptualization of this systematic review; the search strategy and criteria for selection of the literature were designed and implemented by F.M.A. and I.B.H.; data extraction from the chosen literature was handled by H.N.F. and S.A., while M.A. and F.H. took on the responsibility of assessing the quality of the included studies; the synthesis and analysis of the extracted data were jointly overseen by F.M.A., I.B.H., and H.N.F.; the initial draft of the manuscript was prepared by S.A., I.B.H. and M.A.; subsequent reviews and editing were managed by F.H., H.N.F. and F.M.A.; S.A. and M.A. coordinated the project's administration, with H.N.F., S.A. and F.H. providing overarching supervision. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** No data have been used in this study.

**Conflicts of Interest:** The authors declare no conflict of interest.

### References

1. Alsharif, M.H.; Nordin, R. Evolution towards fifth generation (5G) wireless networks: Current trends and challenges in the deployment of millimetre wave, massive MIMO, and small cells. *Telecommun. Syst.* **2017**, *64*, 617–637. [[CrossRef](#)]
2. Alsulami, M.M.; Akkari, N. The Role of 5G Wireless Networks in the Internet-of-Things (IoT). In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
3. Panwar, N.; Sharma, S.; Singh, A.K. A Survey on 5G: The Next Generation of Mobile Communication. *Phys. Commun.* **2016**, *18*, 64–84. [[CrossRef](#)]
4. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 196–248. [[CrossRef](#)]
5. Yousef Alshunaifi, S.; Mishra, S.; Alshehri, M. Cyber-Attack Detection and Mitigation Using SVM for 5G Network. *Intell. Autom. Soft Comput.* **2022**, *31*, 1. [[CrossRef](#)]
6. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G Security Challenges and Solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [[CrossRef](#)]
7. Haider, N.; Baig, M.Z.; Imran, M. Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, Advantages, and Future Research Trends. *arXiv* **2020**, arXiv:2007.04490.
8. Keserwani, H.; Rastogi, H.; Kurniullah, A.Z.; Janardan, S.K.; Raman, R.; Rathod, V.M.; Gupta, A. Security Enhancement by Identifying Attacks Using Machine Learning for 5G Network. *Int. J. Commun. Netw. Inf. Secur.* **2022**, *14*, 124–141. [[CrossRef](#)]
9. Borgesen, M.E.; Kholidy, H.A. *Evaluating Variant Deep Learning and Machine Learning Approaches for the Detection of Cyberattacks on the Next Generation 5G Systems*; SUNY Polytechnic Institute: New York, NY, USA, 2020.
10. Awaysheh, F.M.; Alazab, M.; Garg, S.; Niyato, D.; Verikoukis, C. Big Data Resource Management & Networks: Taxonomy, Survey, and Future Directions. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2098–2130.
11. Noohani, M.Z.; Magsi, K.U. A review of 5G technology: Architecture, security and wide applications. *Int. Res. J. Eng. Technol. (IRJET)* **2020**, *7*, 3440–3471.
12. Gupta, A.; Jha, R.K. A survey of 5G network: Architecture and emerging technologies. *IEEE Access* **2015**, *3*, 1206–1232. [[CrossRef](#)]
13. Kaloxylas, A. A survey and an analysis of network slicing in 5G networks. *IEEE Commun. Stand. Mag.* **2018**, *2*, 60–65. [[CrossRef](#)]
14. Al-Falahy, N.; Alani, O.Y. Y. Millimetre wave frequency band as a candidate spectrum for 5G network architecture: A survey. *Phys. Commun.* **2019**, *32*, 120–144. [[CrossRef](#)]
15. Zhang, J.; Björnson, E.; Matthaiou, M.; Ng DW, K.; Yang, H.; Love, D.J. Prospective multiple antenna technologies for beyond 5G. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1637–1660. [[CrossRef](#)]
16. Agrawal, J.; Patel, R.; Mor, P.; Dubey, P.; Keller, J. Evolution of mobile communication network: From 1G to 4G. *Int. J. Multidiscip. Curr. Res.* **2015**, *3*, 1100–1103.



17. Vij, S.; Jain, A. 5G: Evolution of a secure mobile technology. In Proceedings of the 2016 3rd international conference on computing for sustainable global development (INDIACom), New Delhi, India, 16–18 March 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 2192–2196.
18. Sutton, A. 5G network architecture. *J. Inst. Telecommun. Prof.* **2018**, *12*, 9–15.
19. Rao, J.; Vrzic, S. Packet Duplication for URLLC in 5G: Architectural Enhancements and Performance Analysis. *IEEE Netw.* **2018**, *32*, 32–40. [[CrossRef](#)]
20. 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**, *8*, 195883–195913. [[CrossRef](#)]
21. Cosovic, M.; Tsitsimelis, A.; Vukobratovic, D.; Matamoros, J.; Anton-Haro, C. 5G mobile cellular networks: Enabling distributed state estimation for smart grids. *IEEE Commun. Mag.* **2017**, *55*, 62–69. [[CrossRef](#)]
22. Prasad KS, V.; Hossain, E.; Bhargava, V.K. Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges. *IEEE Wirel. Commun.* **2017**, *24*, 86–94. [[CrossRef](#)]
23. Zhang, Y.; Chen, M. *Cloud Based 5G Wireless Networks*; Springer International Publishing: Cham, Switzerland, 2016.
24. Huo, Y.; Dong, X.; Xu, W.; Yuen, M. Enabling Multi-Functional 5G and Beyond User Equipment: A Survey and Tutorial. *IEEE Access* **2019**, *7*, 116975–117008. [[CrossRef](#)]
25. Parkvall, S.; Dahlman, E.; Furuskar, A.; Frenne, M. NR: The New 5G Radio Access Technology. *IEEE Commun. Stand. Mag.* **2017**, *1*, 24–30. [[CrossRef](#)]
26. Wei, Z. Message Transmission Based on SBA in 5G Core Network. *Railw. Signal. Commun. Eng./Tielu Tongxin Xinhao Gongcheng Jishu* **2021**, *18*, 54–57.
27. Foukas, X.; Patounas, G.; Elmokashfi, A.; Marina, M.K. Network slicing in 5G: Survey and challenges. *IEEE communications magazine* **2017**, *55*, 94–100. [[CrossRef](#)]
28. Hu, Y.C.; Patel, M.; Sabella, D.; Sprecher, N.; Young, V. *Mobile Edge Computing—A Key Technology towards 5G*; ETSI white paper; ETSI: Sophia Antipolis, France, 2015; Volume 11, pp. 1–16.
29. Trivisonno, R.; Guerzoni, R.; Vaishnavi, I.; Soldani, D. SDN-based 5G mobile networks: Architecture, functions, procedures and backward compatibility. *Trans. Emerg. Telecommun. Technol.* **2015**, *26*, 82–92. [[CrossRef](#)]
30. Bairagi, A.K.; Munir, M.S.; Alsenwi, M.; Tran, N.H.; Alshamrani, S.S.; Masud, M.; Hong, C.S. Coexistence mechanism between eMBB and uRLLC in 5G wireless networks. *IEEE Trans. Commun.* **2020**, *69*, 1736–1749. [[CrossRef](#)]
31. Osseiran, A.; Monserrat, J.F.; Marsch, P. (Eds.) *5G Mobile and Wireless Communications Technology*; Cambridge University Press: Cambridge, UK, 2016.
32. Li, Z.; Uusitalo, M.A.; Shariatmadari, H.; Singh, B. 5G URLLC: Design Challenges and System Concepts. In Proceedings of the 2018 15th International Symposium on Wireless Communication Systems (ISWCS), Lisbon, Portugal, 28–31 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
33. Liberg, O.; Sundberg, M.; Wang, E.; Bergman, J.; Sachs, J.; Wikström, G. Cellular internet of things: From massive deployments to critical 5G applications. Academic Press: Cambridge, MA, USA, 2019.
34. Heidari, H.; Onireti, O.; Das, R.; Imran, M. Energy harvesting and power management for IoT devices in the 5G era. *IEEE Commun. Mag.* **2021**, *59*, 91–97. [[CrossRef](#)]
35. Available online: <https://www.enisa.europa.eu/news/enisa-news/enisa-draws-threat-landscape-of-5g-networks> (accessed on 10 September 2023).
36. Pencheva, E.; Nametkov, A.; Velkova, D.; Trifonov, V. 5G System Support for Mission Critical Communications. In Proceedings of the ICEST 2019, Ohrid, North Macedonia, 27–29 June 2019.
37. Dutta, A.; Hammad, E. 5G security challenges and opportunities: A system approach. In Proceedings of the 2020 IEEE 3rd 5G world forum (5GWF), Bangalore, India, 10–12 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 109–114.
38. Jover, R.P.; Marojevic, V. Security and protocol exploit analysis of the 5G specifications. *IEEE Access* **2019**, *7*, 24956–24963. [[CrossRef](#)]
39. Saha, T.; Aaraj, N.; Jha, N.K. Machine learning assisted security analysis of 5g-network-connected systems. *IEEE Trans. Emerg. Top. Comput.* **2022**, *10*, 2006–2024. [[CrossRef](#)]
40. Wu, Y.; Singh, S.; Taleb, T.; Roy, A.; Dhillon, H.S.; Kanagarathinam, M.R.; De, A. (Eds.) *6G Mobile Wireless Networks*; Springer: Berlin, Germany, 2021.
41. Shahraki, A.; Abbasi, M.; Piran, M.J.; Taherkordi, A. A comprehensive survey on 6G networks: Applications, core services, enabling technologies, and future challenges. *arXiv* **2021**, arXiv:2101.12475.
42. Nguyen, V.L.; Lin, P.C.; Cheng, B.C.; Hwang, R.H.; Lin, Y.D. Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [[CrossRef](#)]
43. Shen, S.; Yu, C.; Zhang, K.; Ni, J.; Ci, S. Adaptive and dynamic security in AI-empowered 6G: From an energy efficiency perspective. *IEEE Commun. Stand. Mag.* **2021**, *5*, 80–88. [[CrossRef](#)]
44. Tang, F.; Kawamoto, Y.; Kato, N.; Liu, J. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. *Proc. IEEE* **2019**, *108*, 292–307. [[CrossRef](#)]
45. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. AI and 6G security: Opportunities and challenges. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 616–621.

46. Muppavaram, K.; Govathoti, S.; Kamidi, D.; Bhaskar, T. Exploring the Generations: A Comparative Study of Mobile Technology from 1G to 5G. *Int. J. Electron. Commun. Eng.* **2023**, *10*, 54–62. [[CrossRef](#)]
47. Jasim, K.F.; Al-Shaikhli, I.F. Mobile technology generations and cryptographic algorithms: Analysis study. In Proceedings of the 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia, 8–10 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 50–55.
48. Baraković, S.; Kurtović, E.; Božanović, O.; Mirojević, A.; Ljevaković, S.; Jokić, A.; Husić, J.B. Security issues in wireless networks: An overview. In Proceedings of the 2016 XI International Symposium on Telecommunications (BIHTEL), Sarajevo, Bosnia and Herzegovina, 24–26 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
49. Park, Y.; Park, T. A survey of security threats on 4G networks. In Proceedings of the 2007 IEEE Globecom workshops, Washington, DC, USA, 26–30 November 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 1–6.
50. Han, C.K.; Choi, H.K. Security analysis of handover key management in 4G LTE/SAE networks. *IEEE Trans. Mob. Comput.* **2012**, *13*, 457–468. [[CrossRef](#)]
51. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. 5G security: Analysis of threats and solutions. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 193–199.
52. Mazurczyk, W.; Bisson, P.; Jover, R.P.; Nakao, K.; Cabaj, K. Challenges and novel solutions for 5G network security, privacy and trust. *IEEE Wirel. Commun.* **2020**, *27*, 6–7. [[CrossRef](#)]
53. Qiu, Q.; Liu, S.; Xu, S.; Yu, S. Study on Security and Privacy in 5G-Enabled Applications. *Wireless Commun. Mob. Comput.* **2020**, *2020*, 1–15.
54. Xiang, W.; Zheng, K.; Shen, X.S. (Eds.) *5G Mobile Communications*; Springer: Berlin/Heidelberg, Germany, 2016.
55. Farroha, B.S.; Farroha, D.L.; Farroha, J.S. Analyzing the architecture advantages and vulnerabilities in heterogeneous 5G wireless networks. In Proceedings of the 2019 IEEE International Systems Conference (SysCon), Orlando, FL, USA, 8–11 April 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–8.
56. Mathew, A. Network slicing in 5G and the security concerns. In Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 11–13 March 2020; pp. 75–78.
57. Wijethilaka, S.; Liyanage, M. Survey on network slicing for Internet of Things realization in 5G networks. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 957–994. [[CrossRef](#)]
58. Salahdine, F.; Liu, Q.; Han, T. Towards secure and intelligent network slicing for 5g networks. *IEEE Open J. Comput. Soc.* **2022**, *3*, 23–38. [[CrossRef](#)]
59. Wu, T.Y.; Jie, T.F. 5G Network Slicing Security. In *Advances in Computing, Informatics, Networking and Cybersecurity: A Book Honoring Professor Mohammad S. Obaidat's Significant Scientific Contributions*; Springer International Publishing: Cham, Switzerland, 2022; pp. 755–780.
60. Basin, D.; Dreier, J.; Hirschi, L.; Radomirovic, S.; Sasse, R.; Stettler, V. A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 15–19 October 2018; pp. 1383–1396.
61. Behrad, S.; Bertin, E.; Crespi, N. A survey on authentication access control for mobile networks: From 4G to, 5G. *Ann. Telecommun.* **2019**, *74*, 593–603. [[CrossRef](#)]
62. Sharma, A.; Jain, A.; Sharma, I. Exposing the security weaknesses of fifth generation handover communication. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
63. El Idrissi, Y.E.H.; Zahid, N.; Jedra, M. An efficient authentication protocol for 5G heterogeneous networks. In *Proceedings of the Ubiquitous Networking: Third International Symposium, UNet 2017, Casablanca, Morocco, 9–12 May 2017*; Revised Selected Papers 3; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 496–508.
64. Liyanage, M.; Salo, J.; Braeken, A.; Kumar, T.; Seneviratne, S.; Ylianttila, M. 5G privacy: Scenarios and solutions. In Proceedings of the 2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, USA, 9–11 July 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 197–203.
65. Hu, J.; Li, Z.; Li, P.; Liu, J. A Lightweight and Secure Authentication Protocol for 5G mMTC. In Proceedings of the 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom), Xi'an, China, 25–27 June 2022; pp. 195–200.
66. Chan, W.M.; Kwon, H.M.; Chou, R.A.; Love, D.J.; Fahmy, S.; Hussain, S.R.; Kim, S.W.; Vander Valk, C.; Brinton, C.G.; Marojevic, V.; et al. Adaptive Frequency Hopping for 5G New Radio mMTC Security. In Proceedings of the 2023 IEEE International Conference on Industrial Technology (ICIT), Orlando FL, USA, 4–6 April 2023; pp. 1–5.
67. Salva-Garcia, P.; Chirevella-Perez, E.; Bernabe, J.B.; Alcaraz-Calero, J.M.; Wang, Q. Towards automatic deployment of virtual firewalls to support secure mMTC in 5G networks. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April 2019–2 May 2019; pp. 385–390.
68. Sha, K.; Yang, T.A.; Wei, W.; Davari, S. A survey of edge computing-based designs for IoT security. *Digit. Commun. Netw.* **2020**, *6*, 195–202. [[CrossRef](#)]
69. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access* **2018**, *6*, 18209–18237. [[CrossRef](#)]

70. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge computing security: State of the art and challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [[CrossRef](#)]
71. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [[CrossRef](#)]
72. Kaplanis, C. Detection and prevention of man in the middle attacks in Wi-Fi technology. Doctoral Dissertation, Aalborg University, Aalborg, Denmark, 2015.
73. Mitev, M.; Chorti, A.; Belmega, E.V.; Reed, M. Man-in-the-middle and denial of service attacks in wireless secret key generation. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
74. Al Hayajneh, A.; Alam Bhuiyan, Z.; McAndrew, I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers* **2020**, *9*, 8. [[CrossRef](#)]
75. Hasneen, J.; Sadique, K.M. A survey on 5G architecture and security scopes in SDN and NFV. In *Applied Information Processing Systems. Advances in Intelligent Systems and Computing*; Springer Singapore: Singapore, 2022; pp. 447–460.
76. Jasim, K.F.; Ghafoor, K.Z.; Maghdid, H.S. Analysis of Encryption Algorithms Proposed for Data Security in 4G and 5G Generations. In *ITM Web of Conferences*; EDP Sciences: Les Ulis, France, 2022; Volume 42, p. 01004.
77. Valero, J.M.J.; Sánchez, P.M.S.; Lekidis, A.; Martins, P.; Diogo, P.; Pérez, M.G.; Pérez, G.M. Trusted Execution Environment-enabled platform for 5G security and privacy enhancement. In *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions*; Springer: Cham, Switzerland, 2022; pp. 203–223.
78. Mavoungou, S.; Kaddoum, G.; Taha, M.; Matar, G. Survey on threats and attacks on mobile networks. *IEEE Access* **2016**, *4*, 4543–4572. [[CrossRef](#)]
79. Bendale, S.P.; Prasad, J.R. Security threats and challenges in future mobile wireless networks. In Proceedings of the 2018 IEEE global conference on wireless computing and networking (GCWCN), Lonavala, India, 23–24 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 146–150.
80. Available online: <https://www.digi.com/blog/post/5g-network-architecture> (accessed on 10 September 2023).
81. Arfaoui, G.; Bisson, P.; Blom, R.; Borgaonkar, R.; Englund, H.; Félix, E.; Zahariiev, A. A security architecture for 5G networks. *IEEE Access* **2018**, *6*, 22466–22479. [[CrossRef](#)]
82. Wehbe, N.; Alameddine, H.A.; Pourzandi, M.; Bou-Harb, E.; Assi, C. A Security Assessment of HTTP/2 Usage in 5G Service-Based Architecture. *IEEE Commun. Mag.* **2022**, *61*, 48–54. [[CrossRef](#)]
83. Kim, H. 5G core network security issues attack classification from network protocol perspective. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 1–15.
84. Shaik, A.; Borgaonkar, R.; Park, S.; Seifert, J.P. New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 221–231.
85. Fonyi, S. Overview of 5G security and vulnerabilities. *Cyber Def. Rev.* **2020**, *5*, 117–134.
86. Soldani, D. 5G and the Future of Security in ICT. In Proceedings of the 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand, 27–29 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–8.
87. Moudoud, H.; Khoukhi, L.; Cherkaoui, S. Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT. *IEEE Network* **2020**, *35*, 194–201. [[CrossRef](#)]
88. Lee, J.; Kim, H.; Park, C.; Kim, Y.; Park, J.G. AI-based Network Security Enhancement for 5G Industrial Internet of Things Environments. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19 October 2022; pp. 971–975.
89. Javed, M.A.; Niazi, S.k. 5G security artifacts (DoS/DDoS and authentication). In Proceedings of the 2019 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 20–21 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 127–133.
90. Dehnel-Wild, M.; Cremers, C. *Security Vulnerability in 5G-AKA Draft*; Tech. Rep.; Department of Computer Science, University of Oxford: Oxford, UK, 2018; pp. 14–37.
91. Kodinariya, T.M.; Makwana, P.R. Review on determining number of Cluster in K-Means Clustering. *Int. J.* **2013**, *1*, 90–95.
92. Giles, K.; Hartmann, K. Emergence of 5G Networks and Implications for Cyber Conflict. In Proceedings of the 2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon), Tallinn, Estonia, 31 May–3 June 2022; IEEE: Piscataway, NJ, USA, 2022; Volume 700, pp. 405–419.
93. Huang, H.; Chu, J.; Cheng, X. Trend analysis and countermeasure research of DDoS attack under 5G network. In Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), Zhuhai, China, 8–10 January 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 153–160.
94. Aladwan, M.N.; Awaysheh, F.M.; Alawadi, S.; Alazab, M.; Pena, T.F.; Cabaleiro, J.C. TrustE-VC: Trustworthy Evaluation Framework for Industrial Connected Vehicles in the Cloud. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6203–6213. [[CrossRef](#)]
95. Awaysheh, F.M.; Aladwan, M.N.; Alazab, M.; Alawadi, S.; Cabaleiro, J.C.; Pena, T.F. Security by Design for Big Data Frameworks Over Cloud Computing. *IEEE Trans. Eng. Manag.* **2021**, *69*, 3676–3693. [[CrossRef](#)]

96. Shah, Y.; Chelvachandran, N.; Kendzierskyj, S.; Jahankhani, H.; Janoso, R. 5G Cybersecurity Vulnerabilities with IoT and Smart Societies. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*; Springer: Cham, Switzerland, 2020; pp. 159–176.
97. Cheng, X.; Luo, Q.; Pan, Y.; Li, Z.; Zhang, J.; Chen, B. Predicting the APT for cyber situation comprehension in 5G-enabled IoT scenarios based on differentially private federated learning. *Secur. Commun. Netw.* **2021**, *2021*, 1–14. [[CrossRef](#)]
98. Fang, D.; Qian, Y. 5G wireless security and privacy: Architecture and flexible mechanisms. *IEEE Veh. Technol. Mag.* **2020**, *15*, 58–64. [[CrossRef](#)]
99. Hakak, S.; Gadekallu, T.R.; Maddikunta, P.K.R.; Ramu, S.P.; Parimala, M.; De Alwis, C.; Liyanage, M. Autonomous Vehicles in 5G and beyond: A Survey. *Veh. Commun.* **2023**, *39*, 100551. [[CrossRef](#)]
100. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [[CrossRef](#)]
101. Ali, S.; Haider, A.; Rahman, M.; Sohail, M.; Zikria, Y.B. Deep learning (DL) based joint resource allocation and RRH association in 5G-multi-tier networks. *IEEE Access* **2021**, *9*, 118357–118366. [[CrossRef](#)]
102. Lin, C.C.; Tsai, C.T.; Liu, Y.L.; Chang, T.T.; Chang, Y.S. Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges. *Mob. Netw. Appl.* **2023**, 1–16. [[CrossRef](#)]
103. Xu, Y.; Wang, M.; Zhong, H.; Cui, J.; Liu, L.; Franqueira, V.N. Verifiable public key encryption scheme with equality test in 5G networks. *IEEE Access* **2017**, *5*, 12702–12713. [[CrossRef](#)]
104. Feng, H.; Li, H.; Pan, X.; Zhao, Z.; Cactilab, T. A Formal Analysis of the FIDO UAF Protocol. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2021, Virtua, 21–25 February 2021.
105. Kuadey, N.A.E.; Maale, G.T.; Kwantwi, T.; Sun, G.; Liu, G. DeepSecure: Detection of distributed denial of service attacks on 5G network slicing—Deep learning approach. *IEEE Wirel. Commun. Lett.* **2021**, *11*, 488–492. [[CrossRef](#)]
106. Mu, J.; Jing, X.; Zhang, Y.; Gong, Y.; Zhang, R.; Zhang, F. Machine learning-based 5g ran slicing for broadcasting services. *IEEE Trans. Broadcast.* **2021**, *68*, 295–304. [[CrossRef](#)]
107. Bedari, A.; Wang, S.; Yang, W. A Secure Online Fingerprint Authentication System for Industrial IoT Devices over 5G Networks. *Sensors* **2022**, *22*, 7609. [[CrossRef](#)]
108. Boukerche, A.; Zhang, Q. Countermeasures against worm spreading: A new challenge for vehicular networks. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–25. [[CrossRef](#)]
109. Fourati, H.; Maaloul, R.; Chaari, L. A survey of 5G network systems: Challenges and machine learning approaches. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 385–431. [[CrossRef](#)]
110. Morocho-Cayamcela, M.E.; Lee, H.; Lim, W. Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions. *IEEE Access* **2019**, *7*, 137184–137206. [[CrossRef](#)]
111. Asghar, M.Z.; Abbas, M.; Zeeshan, K.; Kotilainen, P.; Hämäläinen, T. Assessment of deep learning methodology for self-organizing 5g networks. *Appl. Sci.* **2019**, *9*, 2975. [[CrossRef](#)]
112. Khandelwal, A. Artificial Intelligence and Machine Learning Solutions to Network Security in 5G. In *Conference Proceedings of Management & IT*; IIMT: Meerut, India, 2022; p. 102.
113. Kaur, J.; Khan, M.A.; Iftikhar, M.; Imran, M.; Haq, Q.E.U. Machine learning techniques for 5G and beyond. *IEEE Access* **2021**, *9*, 23472–23488. [[CrossRef](#)]
114. Anand, A.; Rani, S.; Anand, D.; Aljahdali, H.M.; Kerr, D. An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications. *Sensors* **2021**, *21*, 6346. [[CrossRef](#)]
115. Nassef, O.; Sun, W.; Purmehdi, H.; Tatipamula, M.; Mahmoodi, T. A survey: Distributed Machine Learning for 5G and beyond. *Comput. Netw.* **2022**, *207*, 108820. [[CrossRef](#)]
116. Moore, J.H.; Lamb, J.M.; Brown, N.J.; Vaughan, D.E. A Comparison of Combinatorial Partitioning and Linear Regression for the Detection of Epistatic Effects of the ACE I/D and PAI-1 4G/5G Polymorphisms on Plasma PAI-1 Levels. *Clin. Genet.* **2002**, *62*, 74–79. [[CrossRef](#)] [[PubMed](#)]
117. Peng, C.; Fan, W.; Huang, W.; Zhu, D. A Novel Approach based on Improved Naive Bayes for 5G Air Interface DDoS Detection. In Proceedings of the 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, Scotland, UK, 26–29 March 2023; pp. 1–6. [[CrossRef](#)]
118. Iavich, M.; Iashvili, G.; Avkurova, Z.; Dorozhynskiy, S.; Fesenko, A. Machine Learning Algorithms for 5G Networks Security and the Corresponding Testing Environment. *Differences* **2022**, *1*, 2.
119. Fang, H.; Wang, X.; Tomasin, S. Machine learning for intelligent authentication in 5G and beyond wireless networks. *IEEE Wirel. Commun.* **2019**, *26*, 55–61. [[CrossRef](#)]
120. Lam, J.; Abbas, R. Machine learning based anomaly detection for 5g networks. *arXiv* **2020**, arXiv:2003.03474.
121. Dangi, R.; Jadhav, A.; Choudhary, G.; Dragoni, N.; Mishra, M.K.; Lalwani, P. ML-based 5g network slicing security: A comprehensive survey. *Future Internet* **2022**, *14*, 116. [[CrossRef](#)]
122. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad. Hoc. Networks* **2021**, *123*, 102685. [[CrossRef](#)]
123. Jothiraj, S.; Balu, S. A novel linear SVM-based compressive collaborative spectrum sensing (CCSS) scheme for IoT cognitive 5G network. *Soft Comput.* **2019**, *23*, 8515–8523. [[CrossRef](#)]



124. Kim, C.; Chang, S.Y.; Kim, J.; Lee, D.; Kim, J. Automated, Reliable Zero-day Malware Detection based on Autoencoding Architecture. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 3900–3914. [[CrossRef](#)]
125. Pavani, A.; Kathirvel, A. Machine Learning and Deep Learning Algorithms for Network Data Analytics Function in 5G Cellular Networks. In Proceedings of the 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 26–28 April 2023; pp. 28–33.
126. He, Y.; Kong, M.; Du, C.; Yao, D.; Yu, M. Communication Security Analysis of Intelligent Transportation System Using 5G Internet of Things from the Perspective of Big Data. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2199–2207. [[CrossRef](#)]
127. Hussain, B.; Du, Q.; Sun, B.; Han, Z. Deep learning-based DDoS-attack detection for cyber-physical system over 5G network. *IEEE Trans. Ind. Inform.* **2020**, *17*, 860–870. [[CrossRef](#)]
128. Aladwan, M.; Awaysheh, F.; Cabaleiro, J.; Pena, T.; Alabool, H.; Alazab, M. Common security criteria for vehicular clouds and internet of vehicles evaluation and selection. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security And Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019.
129. Lu, Y.; Liu, L.; Panneerselvam, J.; Yuan, B.; Gu, J.; Antonopoulos, N. A GRU-based prediction framework for intelligent resource management at cloud data centres in the age of 5G. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *6*, 486–498. [[CrossRef](#)]
130. Ferreira, D.; Reis, A.B.; Senna, C.; Sargento, S. A forecasting approach to improve control and management for 5G networks. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1817–1831. [[CrossRef](#)]
131. Radivilova, T.; Kirichenko, L.; Lemeshko, O.; Ageyev, D.; Mulesa, O.; Ilkov, A. Analysis of anomaly detection and identification methods in 5G traffic. In Proceedings of the 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Piscataway, NJ, USA, 22–25 September 2021; IEEE: Piscataway, NJ, USA, 2021; Volume 2, pp. 1108–1113.
132. Thantharate, A.; Paropkari, R.; Walunj, V.; Beard, C.; Kankariya, P. Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond. In Proceedings of the 2020 10th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0852–0857.
133. Lv, Z.; Singh, A.K.; Li, J. Deep learning for security problems in 5G heterogeneous networks. *IEEE Network* **2021**, *35*, 67–73. [[CrossRef](#)]
134. Wang, T.; Wang, S.; Zhou, Z.H. Machine learning for 5G and beyond: From model-based to data-driven mobile wireless networks. *China Commun.* **2019**, *16*, 165–175.
135. Ly, A.; Yao, Y.D. A review of deep learning in 5G research: Channel coding, massive MIMO, multiple access, resource allocation, and network security. *IEEE Open J. Commun. Soc.* **2021**, *2*, 396–408. [[CrossRef](#)]
136. Huang, H.; Guo, S.; Gui, G.; Yang, Z.; Zhang, J.; Sari, H.; Adachi, F. Deep learning for physical-layer 5G wireless techniques: Opportunities, challenges and solutions. *IEEE Wirel. Commun.* **2019**, *27*, 214–222. [[CrossRef](#)]
137. Restuccia, F.; Melodia, T. Deep learning at the physical layer: System challenges and applications to 5G and beyond. *IEEE Commun. Mag.* **2020**, *58*, 58–64. [[CrossRef](#)]
138. Ftaimi, A.; Mazri, T. Security of deep learning models in 5G networks: Proposition of security assessment process. In *Networking, Intelligent Systems and Security: Proceedings of the NISS 2021, Kenitra, Morocco, 1–2 April 2021*; Springer Singapore: Singapore, 2022; pp. 393–407.
139. Doan, M.; Zhang, Z. Deep learning in 5G wireless networks-anomaly detections. In Proceedings of the 2020 29th Wireless and Optical Communications Conference (WOCC), Newark, NJ, USA, 1–2 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
140. Yadav, N.; Pande, S.; Khamparia, A.; Gupta, D. Intrusion Detection System on IoT with 5G Network Using Deep Learning. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9304689. [[CrossRef](#)]
141. Kebande, V.R.; Alawadi, S.; Awaysheh, F.M.; Persson, J.A. Active machine learning adversarial attack detection in the user feedback process. *IEEE Access* **2021**, *9*, 36908–36923. [[CrossRef](#)]
142. Rathore, S.; Park, J.H.; Chang, H. Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. *IEEE Access* **2021**, *9*, 90075–90083. [[CrossRef](#)]
143. Ahmed, R.; Chen, Y.; Hassan, B. Deep learning-driven opportunistic spectrum access (OSA) framework for cognitive 5G and beyond 5G (B5G) networks. *Ad. Hoc. Networks* **2021**, *123*, 102632. [[CrossRef](#)]
144. Estrada, C.A.; Fuertes, W.; Cruz, H.O. An implementation of an artifact for security in 5G networks using deep learning methods. *Period. Eng. Nat. Sci.* **2021**, *9*, 603–614. [[CrossRef](#)]
145. Kimura, B.Y.L.; Almeida, J. Deep learning in beyond 5G networks with image-based time-series representation. *arXiv* **2021**, arXiv:2104.08584.
146. Santos, G.L.; Endo, P.T.; Sadok, D.; Kelner, J. When 5G meets deep learning: A systematic review. *Algorithms* **2020**, *13*, 208. [[CrossRef](#)]
147. Gupta, A.; Ghanshala, K.; Joshi, R.C. Machine learning classifier approach with gaussian process, ensemble boosted trees, SVM, and linear regression for 5g signal coverage mapping. *Int. J. Interact. Multimed. Artif. Intell.* **2021**, *6*, 156–163. [[CrossRef](#)]
148. Li, J.; Zhao, Z.; Li, R. Machine Learning-Based IDS for Software-Defined 5G Network. *Iet Netw.* **2018**, *7*, 53–60. [[CrossRef](#)]
149. Sevçican, S.; Turan, M.; Gökarslan, K.; Yilmaz, H.B.; Tugcu, T. Intelligent network data analytics function in 5G cellular networks using machine learning. *J. Commun. Netw.* **2020**, *22*, 269–280. [[CrossRef](#)]



150. Abidi, M.H.; Alkhalefah, H.; Moiduddin, K.; Alazab, M.; Mohammed, M.K.; Ameen, W.; Gadekallu, T.R. Optimal 5G network slicing using machine learning and deep learning concepts. *Comput. Stand. Interfaces* **2021**, *76*, 103518. [[CrossRef](#)]
151. Maimó, L.F.; Clemente, F.J.G.; Pérez, M.G.; Pérez, G.M. On the performance of a deep learning-based anomaly detection system for 5G networks. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCOM/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8.

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.