future internet

MDPI

Review

ML-Based 5G Network Slicing Security: A Comprehensive Survey

Ramraj Dangi [1], Akshay Jadhav [1], Gaurav Choudhary [2], Nicola Dragoni [2,*] and Manas Kumar Mishra [1] and Praveen Lalwani [1]

[1] School of Computing Science and Engineering, VIT Bhopal University, Bhopal 466114, India; ramraj.dangi2019@vitbhopal.ac.in (R.D.); akshayjadhav2020@vitbhopal.ac.in (A.J.); manaskumar.mishra@vitbhopal.ac.in (M.K.M.); praveen.lalwani@vitbhopal.ac.in (P.L.)

[2] DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark, DK-2800 Kongens Lyngby, Denmark; gauch@dtu.dk

* Correspondence: ndra@dtu.dk

Abstract: Fifth-generation networks efficiently support and fulfill the demands of mobile broadband and communication services. There has been a continuing advancement from 4G to 5G networks, with 5G mainly providing the three services of enhanced mobile broadband (eMBB), massive machine type communication (eMTC), and ultra-reliable low-latency services (URLLC). Since it is difficult to provide all of these services on a physical network, the 5G network is partitioned into multiple virtual networks called "slices". These slices customize these unique services and enable the network to be reliable and fulfill the needs of its users. This phenomenon is called network slicing. Security is a critical concern in network slicing as adversaries have evolved to become more competent and often employ new attack strategies. This study focused on the security issues that arise during the network slice lifecycle. Machine learning and deep learning algorithm solutions were applied in the planning and design, construction and deployment, monitoring, fault detection, and security phases of the slices. This paper outlines the 5G network slicing concept, its layers and architectural framework, and the prevention of attacks, threats, and issues that represent how network slicing influences the 5G network. This paper also provides a comparison of existing surveys and maps out taxonomies to illustrate various machine learning solutions for different application parameters and network functions, along with significant contributions to the field.

Keywords: 5G network; network slicing; security; threats; machine learning

Citation: 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. https://doi.org/10.3390/fi14040116

Academic Editor: Athanasios Panagopoulos

Received: 18 March 2022
Accepted: 6 April 2022
Published: 8 April 2022

1. Introduction

With the emergence of new technologies that require advances in networks and communication (including high throughput, low latency, and high reliability), such as the Internet of Things (IoT), augmented reality (AR), and vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication [1], 5G networks satisfy more and more of the needs of consumers. 5G has opened up a wealth of opportunities, thereby allowing for innovation and providing reliability for service providers and consumers. These aspects have led service providers to move toward an era of virtualization and adopt 5G.

5G promises data rates that are 10 to 100 times faster, high coverage, high reliability, low latency, an improved quality of service (QoS), and economically affordable services. Such services and opportunities are growing day by day, which has led to competition among service providers and network operators to deploy 5G and adopt the network slicing phenomenon within the physical network.

5G stands for fifth-generation wireless mobile technology, which offers three diverse services: eMBB, mMTC, and URLLC. eMBB stands for enhanced mobile broadband, which offers a 10 to 100 GBPS peak data rate. eMBB uses macro and small cells to provide a high mobility of up to 500 Kmph and also reduces power consumption. mMTC stands for

massive machine type communication, which provides long-range connectivity with a very low data rate of up to 1 to 100 Kbps. It also provides ultra low-cost machine-to-machine (M2M) communication. URLLC stands for ultra-reliable low-latency communication, which offers ultra-responsive connections between multiple devices with less than 1 ms latency. It also offers 5 ms end-to-end latency between mobiles and base stations. It is ultra-reliable and has a 99.9999% available service, which provides medium data rates of approximately 50 Kbps to 10 Mbps [2].

The 5G network is expected to act as an instigator for market growth. Until 2020, there were 92 commercial networks in 38 countries across the world, with only 150 million 5G subscribers in China and 8 million subscribers in South Korea. Ericsson have forecasted to reach 320 million subscribers in the United States only by 2025 [3]. 5G encourages communication service providers (CSPs) to surpass the subscriber-driven business models, make significant improvements, and re-establish CSPs as digital service providers (DSP) for driving innovations, safety, and productivity across the globe [4]. According to the World Economic Forum, 5G is driving the fourth industrial revolution. Many multinational companies are conducting research on 5G, including Samsung, Huawei, LG, Ericsson, Qualcomm, Nokia, ZTE Corp., NEC Corp., Verizon, Orange, AT&T, and Cisco Systems [5]. The Dallas-based company AT&T covers about 16% of the US Basking Ridge. The ultra-wideband network of the New Jersey-based company Verizon now covers 31 states [6]. Qualcomm claims that by 2035, 5G will be worth USD 13 trillion to goods and service industries across the globe [7]. Since 5G can provide connectivity between millions of devices with a faster data rate than ever before, it is necessary to shift over to 5G to cope with the needs and greed of the market. There are numerous ongoing projects that involve 5G and could impact the world through various sectors, such as robotics, medicine, automotives, agriculture, mining, media, and fashion, comprising projects that include untethered industrial robots, robots on farms, AI in diagnosis, VR in palliative care, virtual patient operation (telesurgery), and AR smart glasses and safety [8].

All of the aforementioned services are difficult to provide on 4G mobile networks or any other traditional networks. To compensate for the physical network and provide network services using limited resources at a low cost and minimum expenditure for the network service providers, it is better to partition the physical network through network slicing. Network slicing is one of the key features of 5G. The idea is to partition the physical network into multiple logical networks, so that each logical network can provide specific services depending on the relevant application and its requirements [9]. Due to the enhancement of the virtualization concept in Cloud computing, there has been an increase in the expansion of physical network resources into multiple logical or virtual networks. These logical or virtual network are called “slices” in 5G jargon. A network slice is a free-standing virtual network with resources, flows, security mechanisms, topology, and a standard and well-defined QoS. These slices are isolated from each other and provide specific services for subscribers according to their demands [10]. Network slicing provides flexibility and scalability by allowing heterogeneous services to run over the shared physical network. It is adaptable to the changes in the requirements of the subscribers and it provides end-to-end communication. It supports the multi-service environment, on-demand network services, and multi-tenancy features within 5G.

1.1. Contributions of This Paper

1. This paper introduces all of the basics of 5G, the current trends of 5G, network slicing, layers within network slicing, and various standardized architectural frameworks (Section 3);
2. The paper also provides a state-of-the-art comparison and map of existing related surveys, with an emphasis on their major contributions (Section 2);
3. The paper demonstrates the use of state-of-the-art applied ML algorithms in different stages of network slicing, such as resource allocation and slice admission (Section 4);

4. A taxonomy of attack prevention from the proposed frameworks, services, and security considerations of network slicing.
5. The paper also discusses machine learning-based network slicing and the ML-based techniques that can be applied during different stages of slicing to prevent attacks over the network.
6. The paper discusses network slicing threats and their countermeasures throughout the complete lifecycle of a network slice.
7. Finally, the paper outlines ongoing research on and future directions for 5G network slicing security to enable 5G to become more secure and robust without affecting network and end-user connectivity (Section 7).

1.2. Outline of the Survey

The rest of the paper is structured as follows: Section 2 contains a state-of-art comparison of existing surveys and road-maps. Sections 3 and 4 discuss network slicing and its paradigms and various machine learning-based network slicing along with taxonomy, respectively. Sections 5 and 6 include the emerging threats and security concerns, the taxonomy of network slicing attack prevention, and network slicing security solution and management, respectively. Section 7 consists of recommendations and future directions. Section 8 concludes the paper. This review paper also helps the future perspective and ideas among researchers. A graphical representation of the paper's organization is depicted in Figure 1. We include the definition of frequently used acronyms in Table 1.

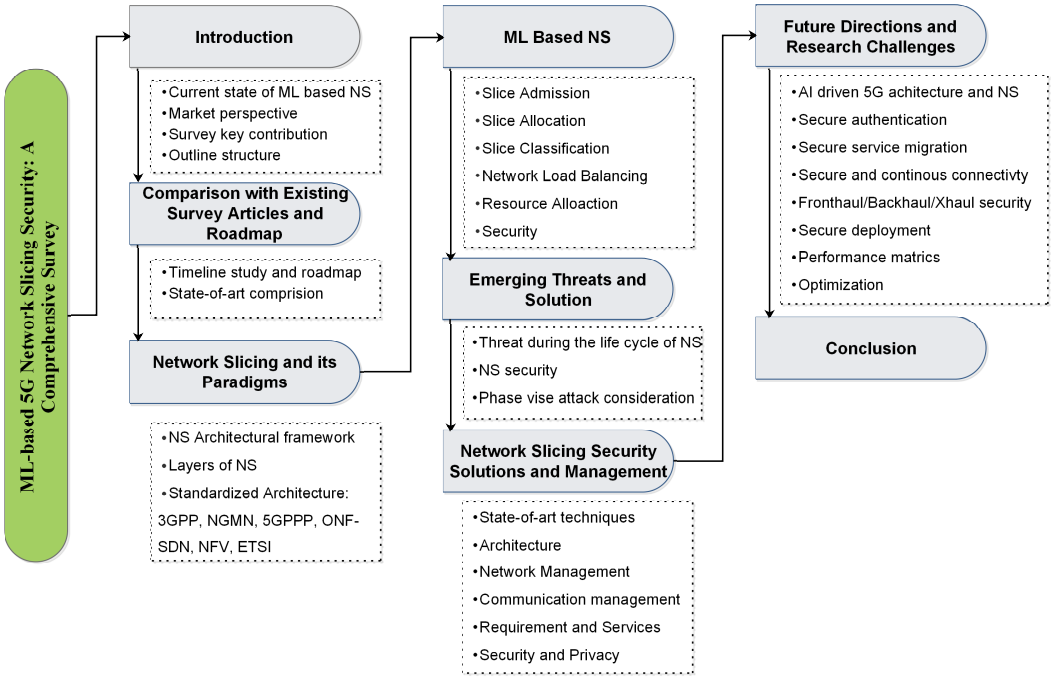

Figure 1. Systematic layout representation of this survey.

Table 1. Summary of acronyms.

Abbreviations	Full Forms	Abbreviations	Full Forms
3GPP	Third Generation Partnership Project	**MEC**	Multi-Access Edge Computing
5G	Fifth Generation Wireless Network	**ML**	Machine Learning
5GC	Fifth Generation Core	**MME**	Mobility Management Entity
5GPPP	Fifth Generation Infrastructure Public Private Partnership	**mMIMO**	Massive Multi Input Multi Output
AI	Artificial Intelligence	**mMTC**	Massive Machine Type Communication
APIs	Application Programmable Interfaces	**mmWAVE**	millimeter WAVE
AR	Augmented Reality	**NFV**	Network Function virtualization
BBU	BaseBand Units	**NFVI**	NFV Infrastructure
C-RAN	Centralised Radio Access Network	**NGMN**	Next Generation Mobile Network Alliance's
CN	Core Network	**NMS**	Network Management System
CSP	Communication Service Providers	**NN**	Neural Network
D-RAN	Distributed Radio Access Network	**NS**	Network Slicing
D2D	Device to Device	**NS3**	Network Simulator 3
DBN	Deep Belief Network	**ONF**	Open Network Foundation
DDoS	Distributed Denial of Service	**OSS/BSS**	Operation/Business Support System
DL	Deep Learning	**OWFE**	Optimal Weight Feature Extraction
DoS	Denial of Service	**PDN-GW**	Packet Data Network Gateway
DRL	Deep Reinforcement Learning	**QoE**	Quality of Experience
DSP	Digital Service Providers	**QoS**	Quality of Service
E2E	End to End	**RAN**	Radio Access Network
eMBB	Enhanced Mobile Broadband	**RRH**	Radio Remote Heads
eMTC	Enhanced Machine Type Communication	**S-GW**	Serving Gateway
ETSI	European Telecommunications Standards Institute	**SDN**	Software Defined Networking
GS-DHOA	Glowworm Swarm-based Deer Hunting Optimization Algorithm	**SLA**	Service Level Agreement
HSS	Home Subscriber Server	**SONs**	Self Organising Networks
IDS	Intrusion Detection System	**SSIDs**	Service Set Identifiers
IETF	Internet Engineering Task Force	**SVM**	Support Vector Machine
InPs	Infrastructure Providers	**TS**	Technical Specifications
IoT	Internet of Things	**UCON**	Usage Control Mechanism
kNN	k Nearest Neighbors	**UltraHD**	Ultra High Definition
KPIs	Key Programmable Interface	**URLLC**	Ultra-Reliable Low Latency Communication
LTE	Long Term Evolution	**V2V**	Vehicle-to-Vehicle
LTE-A	Long Term Evolution-Advance	**V2X**	Vehicle-to-Everything
M2M	Machine to Machine	**VNF**	Virtualized Network Functions
MANO	Management and Orchestration	**VR**	Virtual Reality

2. Comparison with Existing Survey Articles and Roadmap

Some studies emphasize network slicing in some aspects such as SDN, NFV, security solutions, attacks over a network. Table 2 incorporates a summary of existing surveys on network slicing. Barakabitze et al. [11] give some updated solutions in NS using SDN and NFV. Kaloxylos [12] covers domains such as transport, accessibility in the slices. Qiang et al. [13] show the importance of SDN and NFV in overcoming the traditional problems in the network. Zhang [14] discussed the concept of modularization and dynamic service chaining concerning NFV. Finally, Zhang et al. [15] provide a study on E2E slicing models.

Table 2. Comparison with existing survey articles and road-maps (discussed: ✓ never mentioned: - partially mentioned: *).

Authors	Main Contribution	SDN and NFV Based NS	ML Based NS	Threats and Attacks	Security Solutions	Research Challenges
[11]	Author contributed a comprehensive survey with updated solutions related to 5G NS using SDN and NFV.	✓	-	✓	✓	ML based NS is not covered
[12]	This survey covers solutions for network slicing domains such as access, transport and core.	✓	-	-	✓	ML based NS and security considerations are not covered
[13]	The author contributed the importance of SDN and NFV, to overcome the traditional problems in the network.	✓	-	-	✓	ML based NS and security considerations are not covered
[14]	The author discussed the key technologies such as NFV, modularisation, dynamic service chaining, and MANO.	✓	-	-	✓	ML based NS and security considerations are not covered
[15]	This survey provided a study on End to End network slicing model to enable Smart Grid.	✓	-	-	-	ML based NS, threats and security considerations not discussed.
[16]	The survey mainly focuses on applications of 5G. Additionally, emphasize ETSI architecture with capabilities of SDN and NFV.	✓	-	-	✓	ML base NS and threats are not discussed in the study.
[17]	The author discussed the network slicing and its architecture, services along with the challenges.	✓	-	-	-	ML based NS, threats and security considerations not discussed.
[18]	The article mainly focuses on principles and models of resource allocation in NS. Additionally, categorised the mathematical model of resource allocation.	✓	-	-	✓	ML base NS and threats are not discussed in the study.
[19]	The author discussed the challenges and open issues regarding resource allocation and isolation in slices.	✓	-	-	✓	Discussed a fact that machine learning techniques can be considered to learn control policies in wireless networks.
[20]	The article focuses on the advancement of network slicing in IoT and smart applications. Additionally, discussed the key requirements to enable smart services.	✓	✓	-	✓	Recommended machine learning approaches for future research.
[21]	The survey emphasises on Software defined IoT orchestration using Edge computing to solve the challenges in IoT service management.	✓	*	✓	✓	Discussed the use of machine learning for IoT to prevent malicious attacks, traffic and to manage user requests.
[22]	The author discussed the end-to-end network slicing along with the enabling technologies and solutions. Additionally, explained how slicing can be achieved while considering RAN sharing and the core network.	✓	-	-	✓	ML base NS and threats are not discussed in the study.
[23]	This article discussed the utilization of NS in IoT applications, along with the obstacles in network slicing which occurs due to the advancement of the IoT.	-	✓	✓	✓	Recommended ML for future research direction in terms of NS and IoT.
This Survey	This survey incorporates the basics of network slicing, services, and the threats associated along with the attacks. Additionally, includes the machine learning approaches and solutions based on the stages in the network slice lifecycle.	✓	✓	✓	✓	ML base NS concepts, threats, and attacks are discussed in the study. Research challenges- AI driven 5G architecture and network slicing, Secure authentication, Secure service migration, Fronthaul/Backhaul/Xhaul Security is covered.

Some surveys focus on the architecture and challenges in the NS. Lucena et al. [16] emphasized 5G architecture along with the capabilities of SDN, NFV, and the application of 5G. Foukas et al. [17] discuss the challenges of NS and its architecture. Su et al. [18] and Richart et al. [19] focused on resource allocation in slices. Khan et al. [20] and Wijethilaka et al. [23] discussed the advancement of the NS in IoT and smart applications, as well as challenges in NS due to the evolution of IoT. Rafique et al. [21] give solutions to the challenges in IoT service management. Afolabi et al. [22] explained how slicing can be achieved in RAN and CN networks along with the enabling technologies and solutions.

These surveys emphasized NS and provided solutions to the issues but lacked machine learning-based Network Slicing. Some studies recommended ML approaches for future research to counter these challenges. Our survey mainly emphasizes Machine Learning-based Network Slicing and new blend-up solutions based on ML, how ML can be applied over various stages in the NS life cycle, and network components and 5G NS application parameters.

Figure 2 shows the evolution of Network Slicing, the year of conceptualization [24], implementation [25,26] network virtualization [27,28] the concept of SDN [29] and NFV [30,31], and different services for the users [32–36]. From the year 2015, research in the field of Network Slicing accelerated, with the result of increasing the quality of services. Various Machine Learning (ML) [37–39] and Deep Learning (DL) [40–44] algorithms are being applied to manage slices, user requests, slice admissions, resources, and traffic in 5G network slicing. Various optimization algorithms [45,46] are also utilized to optimize the network functions.

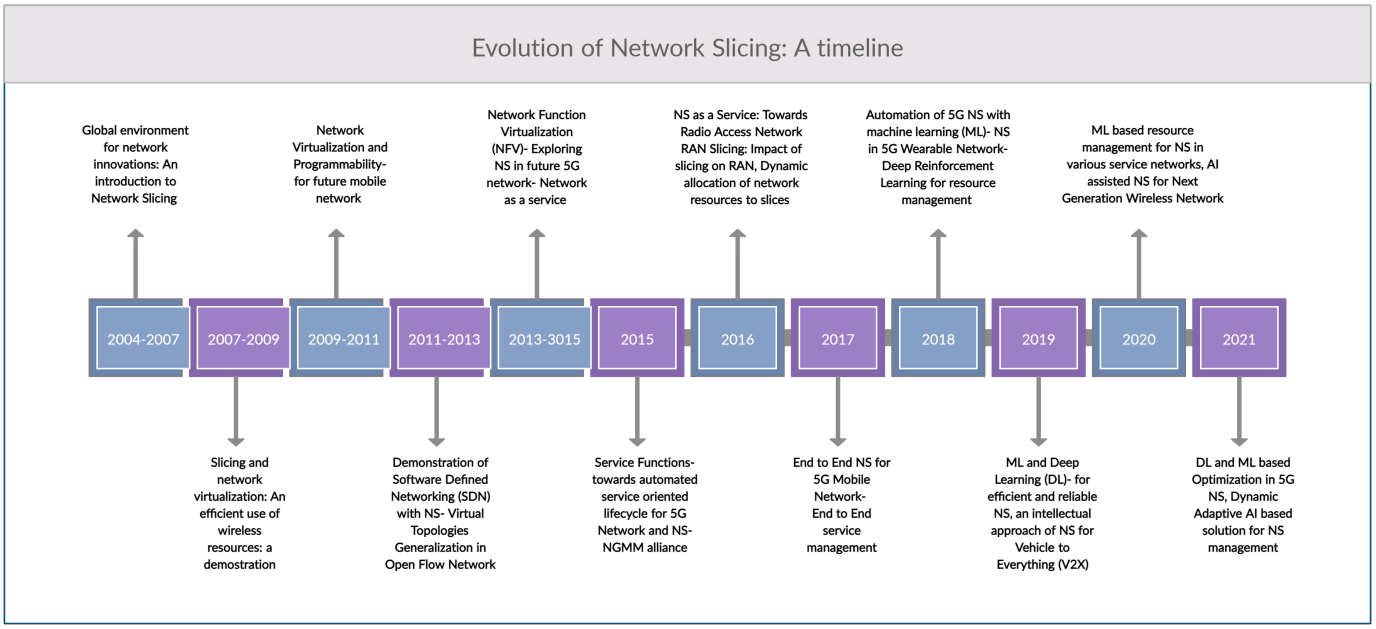

Figure 2. Evolution of network slicing: A timeline.

3. Network Slicing and Its Paradigms

Network slicing is one of the key features of the 5G mobile network, which boosts the performance of complete architecture. 5G differs from 1G to 4G mobile networks; it offers various other services with mobile broadband services such as mMTC and URLLC. To offer multiple heterogeneous services from a single platform which is flexible in nature, the flexibility is provided by a network slicing mechanism in which one physical network is divided into multiple logical networks to offer these services simultaneously. Each network slice creation is done in four phases: softwarization, virtualization, orchestration, and management. These slices use generic resources to serve users and specific applications. SDN and NFV play a significant role in slicing to make the 5G network more scalable

and reliable. Network slicing deals with three prominent use cases: the first enhances mobile broadband (eMBB) for those applications which require high bandwidth to offer Ultra-HD video communication. This use case increases the traffic load on mobile networks. The second massive machine type communication (mMTC) offers connectivity between millions of devices. This use case does not increase traffic but increases the magnitude of mobile networks. The last service is ultra-reliable low latency communication (URLLC) which applies to connectivity, remote surgery, industry 4.0, etc. in vehicles to everything (V2X). This use case needs very low latency connectivity [16].

The network slicing architectural framework is based on three categories, as mentioned in Figure 3.

- Radio Access Network (RAN) slicing: In the 4G network, one extra en-gNB master node is added to benefit the cloudification in the 5G network. The next-generation RAN is dynamic and scalable, adding or releasing the requirement's network functions. It also balances the load over the slice and manages the resources over the slice [47]. Implementation of RAN in network slicing can be done through logical abstraction of physical resources such as base stations (master eNB and secondary en-gNB) packet data network gateway (PDN-GW), home subscriber server (HSS), serving gateway (S-GW), mobility management entity (MME) [48].
- Core Network (CN) slicing: The 4G network works on centralized architecture without a fully isolated control and data plane. The problems with such centralized architectures are its single point of failure and traffic congestion, etc. The core slicing developed in 3GPP isolates the control and data plane, effectively supporting mobile broadband services and massive and mission-critical IoT services. The core network architecture includes the following network functions: access and mobility management functions, authentication server functions, unified data management functions, data storage functions, session management functions, user equipment, user data plane functions, policy control functions, and RAN [49].

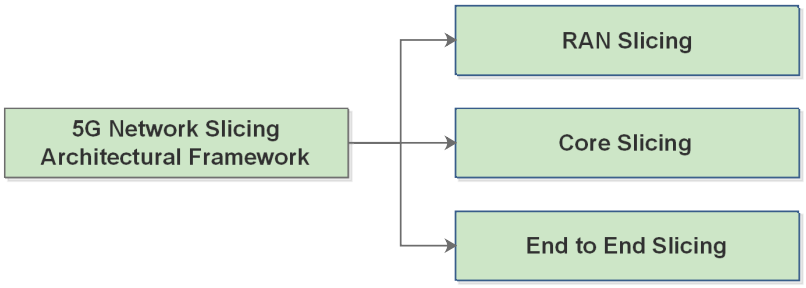

Figure 3. 5G network slicing architectural framework.

Network slicing involves three layers: As shown in Figure 4.

- The Service Instance layer offers the services to the end-user or subscriber based on their request. Each service in the service instance layer is represented as an 'instance'.
- The Network Slice Instance layer includes the network slices, which are customized with all the network features and are provided to the service instance.
- The Resource layer is a pool of all the virtual and physical resources which are required by the network slices to serve the services of the service instance.

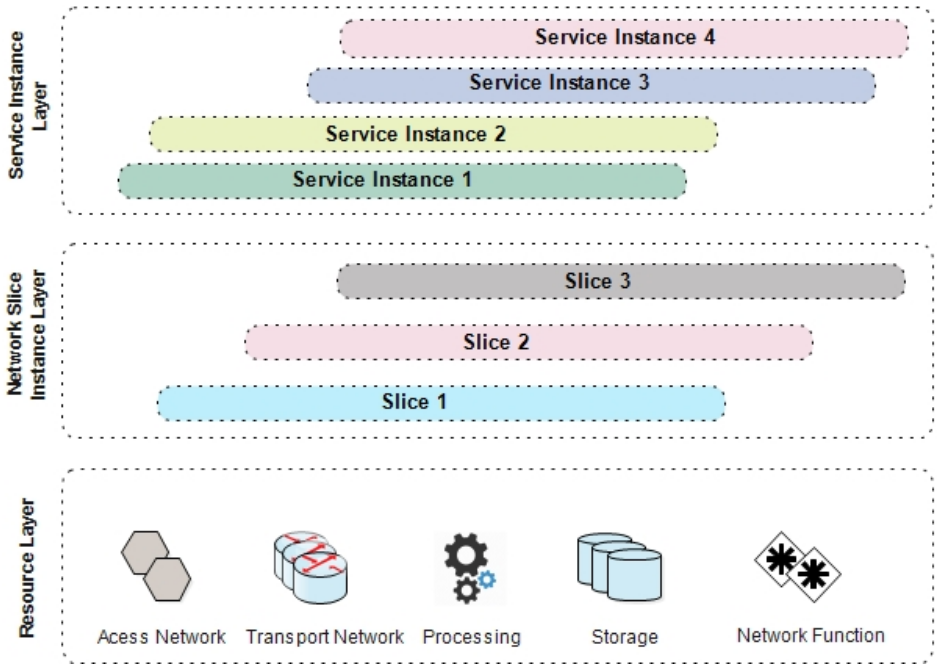

Figure 4. Layers of network slicing.

Architecture

Network Slicing architecture is mainly composed of two blocks: actual slice implementation and slice management and configuration. The first block is responsible for creating slices, allocating resources, and deploying at the end-user level. The other block manages and controls the functionalities and effective mutualism between the slices. Standard bodies provide numerous proposed architectures for network slicing in 5G. Table 3 represents state-of-art studies on various architectural standards by different authors.

Table 3. The state-of-the-art studies by different authors on various architectural standards. 3GPP—3rd Generation Partnership Project, 5G-PPP—5G Infrastructure Public Private Partnership, SDN—Software Defined Networking, NFV—Network Function Virtualization, ETSI—European Telecommunication Standards Institute, NGMN—Next Generation Mobile Networks.

References	3GPP	5G-PPP	SDN	NFV	ETSI	NGMN
[17]		Yes				Yes
[16]			Yes	Yes	Yes	
[12]	Yes					
[14]	Yes					
[47]					Yes	
[50]		Yes				
[51]	Yes			Yes	Yes	
[52]		Yes				
[53]				Yes	Yes	
[54]	Yes					
[22]	Yes	Yes	Yes			Yes
[55]		Yes	Yes	Yes		Yes

3GPP standardized architecture. Saboorian et al. [54] proposed architecture for network slicing based on 3GPP services and system aspects. The authors specified the current architecture is based on the 5G Core (5GC) and described various technical specifications (TS). Some of the TS are as follows: TS 23.501 specifies stage 2 system architecture, TS

23.502 specifies the procedure, and TS 23.503 specifies policy and charging control for 5G network system. Additionally, we suggest that 3GPP collaborates with ETSI and NFV to obtain effortless end-to-end network connectivity and smooth execution of slices in a virtual environment.

NGMN standardized architecture. Next Generation Mobile Network (NGMN) Alliance visualizes the 5G network as an end-to-end system with extreme productivity and feasibility. NGMN comprises both RAN and CN for E2E connectivity. NGMN justifies that the 5G network slicing system must be designed keeping in mind the current trends and principles such as dynamic radio topology and cost-effective deployment to create common composable cores, flexibilities, built-in security, and simplification of operations and management. Foukas et al. [17] break the overall architecture into three layers as shown in Figure 5.

- Infrastructure resource layer—the pool of physical resources such as access nodes, cloud nodes, networking nodes, and 5G supportable devices are constituted at this layer. These resources are disclosed to the upper layers through virtualization.
- Business enablement layer—the library of all modular network functions comprehended by software modules and value-enabling capabilities; a set of configuration parameters such as RAT config. These parameters and functions are called by orchestration entities via APIs.
- Business application layer—comprises applications of the operators, enterprises, verticals, and third-party services that use 5G.

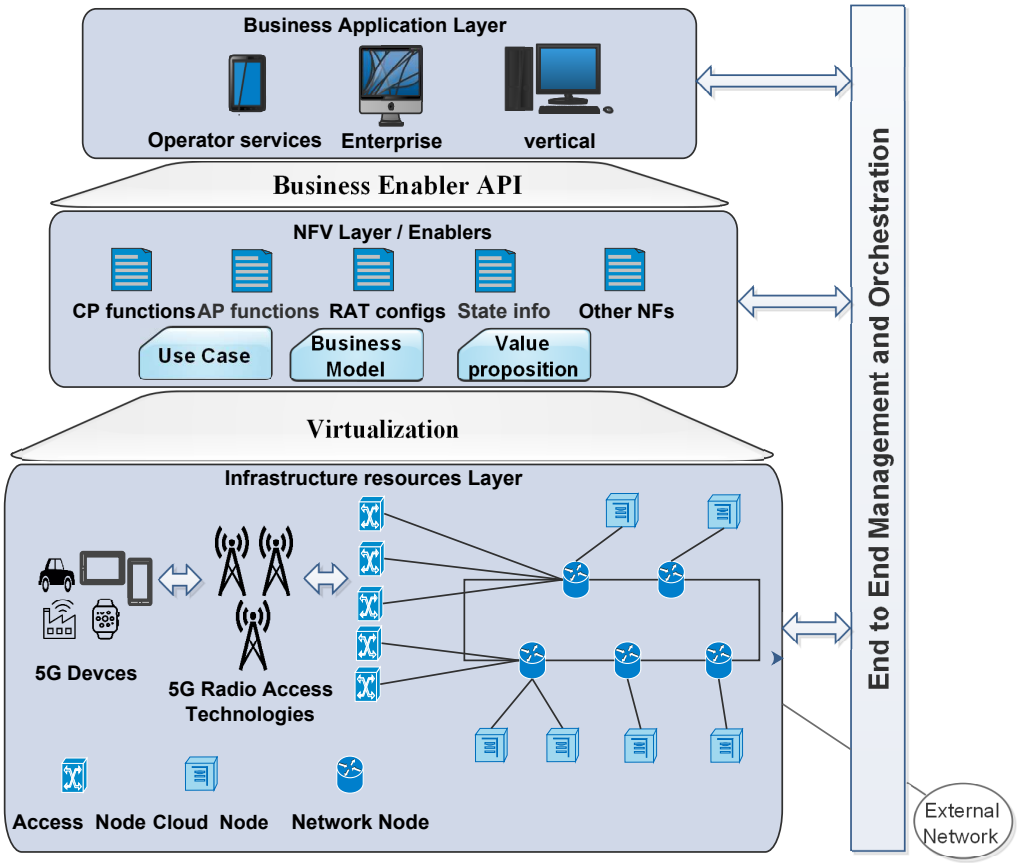

Figure 5. NGMN architecture.

5G-PPP standardized architecture. 5G-PPP expands the roles of the 5G network to support virtualization and softwarization and to encourage slicing for diverse use cases. In comparison to the NGMN architectural proposal of layers, where both architectures are based on the network function and infrastructure layers, 5G-PPP divides the framework

into five layers: infrastructure, network function, orchestration, business function and service layers. Orchestration or MANO is a separate layer and the business application layer of NGMN is separated into two different layers: the business function and service layer in 5G-PPP [17].

ONF-SDN standardized network slicing architecture. Open Network Foundation (ONF) defines orchestration as a selection process of resources and optimally managing the client's request. The orchestrator is governed by an administrative body that tends to follow specific policies and fulfill clients' service requests. The SDN supports the slicing phenomenon, which needs to ensure the clients' service requests are fulfilled effectively and swiftly. The two main components in ONF-SDN architecture are controllers and resources, as shown in Figure 6. The controller mediates between the clients and resources as a centralized body pictured in the control plane. The administrator controls and configures the entire controller, including the client and server context and its policies for effective functioning [16].

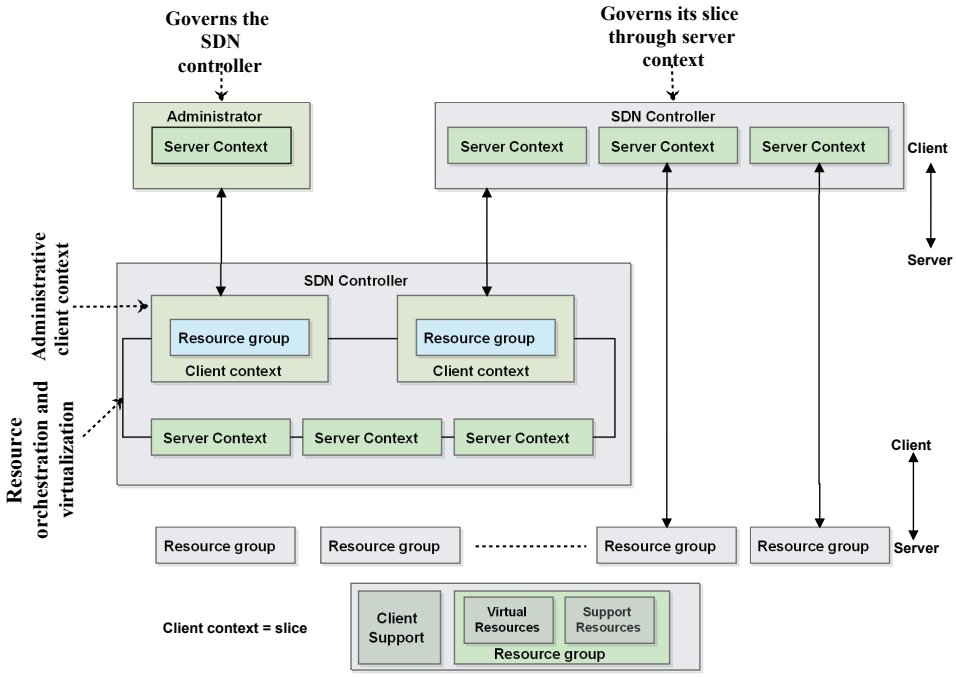

Figure 6. ONF- SDN architecture.

Network Function virtualization (NFV) standardized architecture. ONF-SDN architecture discussed the control plane features that enable network slicing architecture but lack effective management of network slicing and its essential resources. NFV architecture is comprised of the following: NFV Infrastructure (NFVI), a collection of resources; virtual network functions run on NFVI and MANO, consisting of a VNF Manager, Orchestrator and Virtualized Infrastructure Manager; and a Network Management System (NMS), which is comprised of Element Management (EM) and Operation/Business Support Systems (OSS/BSS) [51,56]. The NFV architecture works on the management of infrastructure resources and directs the allocation of the slices concerning the needs of the virtual networks and network services.

ETSI standardized architecture. The European Telecommunications Standards Institute (ETSI) standards led NFV in 2012, and since then, it has collaborated with industries to set up a standard to support the concept of network virtualization. The ETSI standard sets up an architectural framework for NFV; it focuses on the changes in the network which are likely to happen due to the NFV virtualization process. It never focuses on network functions, packet flow, end-to-end network services, or physical infrastructure control.

Instead, it adds new reference points and functional blocks. With NFV, generic hardware can handle the software [12]. ETSI works on three domains, as shown in Figure 7.

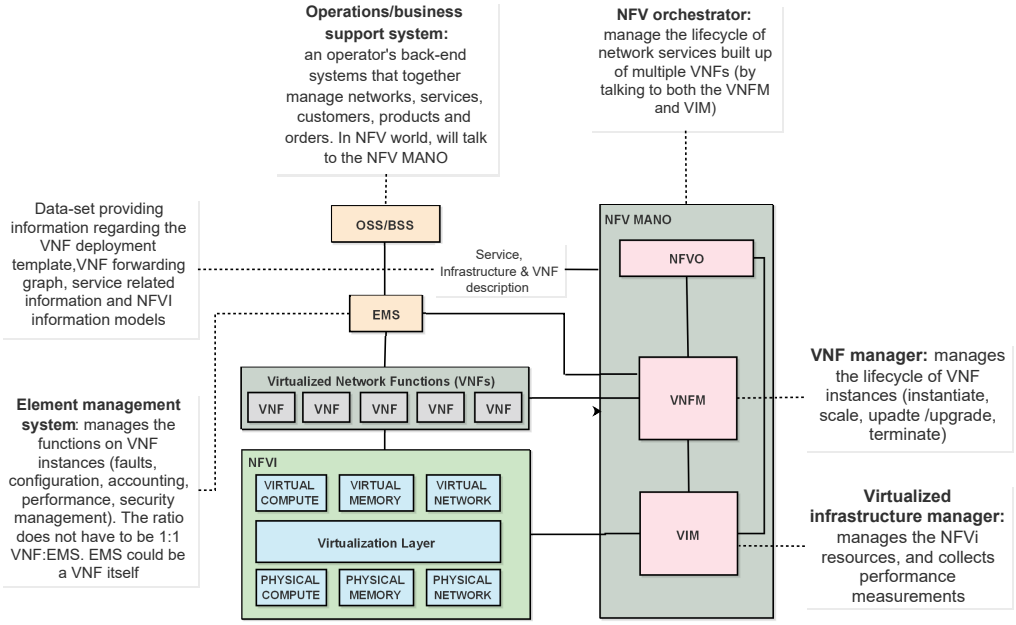

Figure 7. ETSI architecture.

4. Machine Learning Based Network Slicing

Machine Learning (ML) is a branch of Artificial Intelligence (AI) based on the ideology of self-learning, where the machine or the system can self-learn based on the previous results or the dataset gathered with less human intervention. It has the potential to provide more straightforward solutions to complex problems by learning from and analyzing bulk data. It analyses and adapts the changes as per the environment and predicts the near future with accurate results. With the growing amount of data and market competition, ML technology is being adopted by most industries and sectors such as the government, healthcare, retail, financial services, and transportation. By extracting insight from the data, the organizations can work more effectively and procure advantages over the competitors.

5G networks are becoming more complex due to the emergence of an exceptionally massive number of newly connected devices and different types of services that can be termed as data. With the increase in the volume of traffic and service requests for diverse users and applications, there has been an increase in the need for creating network slices over physical networks to optimize the services and the requests by maintaining the robustness, workload, and security in the network with the involvement of ML technologies. ML can be considered an automation in various network operations and management such as planning and design, construction and deployment, on-demand adaptive network configuration, monitoring, fault detection, and security. Figure 8 portrays various network functions in network slicing and their relevant ML techniques. ML also provides algorithms to retrieve information from raw data, perceptive advice, and prediction based on learning [39]. Focusing on machine learning-based network slicing, numerous research has been published to emphasize the use of ML and DL models along with the network components, application parameters, and security considerations, as shown in Table 4.

Table 4. The state-of-the-art ML based available solutions. Z1: Core Network; Z2: Fronthaul; Z3: Backhaul; Z4: Xhaul; Z5: Radio Access Network; LB: Load Balancing; NVF: Network virtualization Function; SDN: Software Defined Networking; RA: Resource Allocation; SEC: Security; HO: Handouts. (Discussed: ✓ Never Mentioned: X).

Authors	Key Contribution	ML Applied	Network Participants Component					5G Network Application Parameters					Security Consideration
			Z1	Z2	Z3	Z4	Z5	LB	NVF	SDN	HO	RA	SEC	
[57]	Resource Scheduling	Deep Reinforcement Learning (DRL)	✓	X	X	X	X	X	✓	✓	X	✓	X	-
[58]	QoS	ML algorithm	✓	X	X	X	✓	X	✓	✓	X	✓	X	-
[40]	Security in Network Slicing	Deep Learning Neural Network (DLNN)	✓	X	X	X	X	✓	✓	✓	X	✓	✓	DLNN: to manage load load efficiency and network availability
[46]	Optimization and Slice prediction	GS-DOHA + NN + DBN	✓	X	X	X	X	X	✓	✓	X	✓	X	-
[59]	Slice Allocation	Random Forest, SVM, kNN, Decision Tree	✓	X	X	X	X	X	✓	✓	X	*	X	-
[60]	Slice Admission	Reinforcement learning	X	✓	✓	X	✓	X	✓	✓	X	✓	X	-
[39]	Automation in Network Function	ML algorithm	✓	X	X	X	X	X	✓	✓	X	✓	✓	Traffic analysis, DPI, threat identification and infection isolation
[43]	Resource Allocation	LSTM	✓	X	X	X	✓	✓	✓	✓	X	✓	X	-
[61]	Identifying mobile applications and enabling application specific Network Slicing	Deep Learning (DL)	X	X	X	X	✓	X	✓	✓	X	X	X	-
[62]	Security in Network Slicing	Deep learning (DL)	✓	X	X	X	✓	✓	✓	✓	X	✓	✓	Secure 5G: to detect and eliminate threats based on incoming connections.
[63]	Cooperative attack detection	Reinforcement learning	✓	X	X	X	✓	X	✓	✓	X	X	✓	To secure end-end network against internal and external attacks
[64]	Designed jamming attack	Reinforcement learning	X	X	X	X	✓	X	X	X	X	✓	✓	To secure network slicing against RL based jamming attacks, they introduced a defense mechanism such as Q-table update.
[65]	To built comprehensive architecture and experimental framework for the future self organising network	Naive Bayes, SVM, NN, GBT and RF	X	X	X	X	✓	X	✓	✓	X	✓	X	-
[66]	Resource Allocation	Unsupervised ML	✓	X	X	X	X	X	✓	✓	X	✓	X	-
[67]	Big-data driven dynamic slicing	ML and DL algorithm	✓	X	X	X	X	X	✓	✓	X	✓	X	-
[68]	Resource allocation for Edge Computing	Deep Reinforcement Learning	✓	X	X	X	X	X	X	X	X	✓	✓	The Blockchain Network Slicing Broker (BNSB) handles requests and manages resource allocation. The Blockchain technology ensures the security of transactions.
[69]	Joint Radio and Cache Resource Allocation	Transfer Reinforcement Learning (TRL)	✓	X	X	X	✓	X	X	X	X	✓	X	-
[70]	Network slicing with diverse resource stipulations and dynamic data traffic	Deep Q Learning	X	X	X	X	✓	X	✓	✓	X	✓	X	-

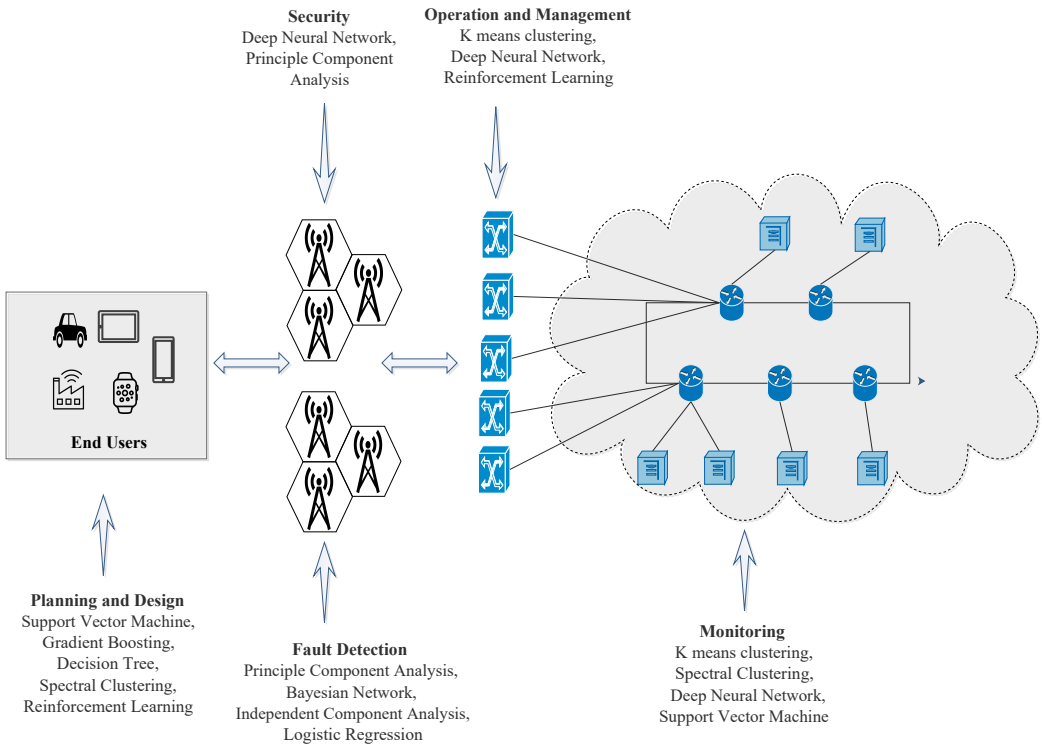

Figure 8. Network functions and relevant ML techniques.

In case of slice admission in the 5G network, infrastructure providers (InPs) have to effectively and efficiently serve a variety of services, improve resource efficiency, and reduce the cost based on the service request, which can be scaled up or scaled down as per the requirements and service time. In such cases, the profit of the InPs can only be increased when they accept as many slice requests as possible and check the variations in the slice's requirements to avoid performance degradation. Here, it is necessary to create an intelligent slice admission scheme for systematic admission; the ML approach can be best suited to preventing the obstruction in the infrastructure and obtaining the maximum profit for an InP. Raza et al. [60] have modeled an ML approach with two algorithms working together, i.e., supervised learning and reinforcement learning. Supervised learning-based big data analytics collected historical data and observed the change in the requirements of the incoming requests and the present slices. In contrast, a reinforcement learning-based solution checks the circumstances where obstruction can occur in the system or infrastructure. From these observations and learning, they only admitted those slices that may not give rise to any obstruction and may not lead to degradation. Consequently, the profit of InPs will rise.

Considering use cases such as throughput, availability, reliability, scalability, and latency in terms of quality of service (QoS) and quality of experience (QoE), respectively, 5G networks tend to provide such flexibility and use cases. Since virtual slice allocation in network slicing over a physical network over a shared pool of resources becomes very complex, an ML-based approach can be modeled to solve this problem. To select the best suitable slice, Gupta et al. [59] use different ML algorithms such as Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Tree over the Unicauca-Version-2 public dataset (7 days data, containing 87 attributes), and simulation performed with an NVIDIA GPU. The results show that slice selection strategy in the Random Forest and KNN algorithms give more accurate results than SVM and Decision Tree algorithms to obtain a high QoS and Service Level Agreement (SLA).

To overcome the challenges which affect the performance of network slicing, various ML and hybrid learning models are applied for effective slicing. Abidi et al. [46] proposed glowworm swarm-based deer hunting optimization algorithms (GS- DHOA), which are two meta-heuristic optimization algorithms. They combined these two algorithms to optimize weight function. First, they collected the data from different 5G networks, with attributes such as device type, bandwidth, duration, modulation type, packet delay, and packet loss ratios. Then they carried out the optimal weight feature extraction (OWFE) using the proposed GS-DHOA model; next, they performed slice classification in which they classified the slices based on eMBB, mMTC, and URLLC with respect to the devices, with the help of a hybrid classifier—a hybrid of Deep Belief Network (DBN) and an NN.

Another approach to making slice selection more efficient and accurate while handling network load balancing and avoiding slice failure is using a Deep Learning NN. The load efficiency, availability, efficient utilization of resources, and network are also to be considered while slicing the selection. A model called DeepSlice uses KPIs to analyze the network traffic and predict the device type. It also manages the efficient use of resources, allocation, and load balancing. It aims for proper selection of slices, slice prediction with adequate resource allocation, traffic management, slice management, and new slice allotment in case of a slice or network failure. Their model also identifies the traffic pattern and predicts the future patterns to avoid forthcoming failure [40].

With the emergence of the 5G network and its popularity and ability to serve an abundance of services, and with the rise in the complexity of the network compared to previous generation networks, ML approaches have become a necessary part of 5G [65]. The self-organizing networks (SONs) in 5G and network slicing need to be integrated with SDN and NFV to build a comprehensive architecture and experimental framework, using ML and Big Data techniques to develop more intelligent capabilities for the future to satisfy the emerging requirements and to assure intelligence, automation, faster management, and optimization [65]. ML approaches have been used to ameliorate network security, as well as access control, authentication, anti-jamming offloading and malware detection in 5G networks to protect users' data and to maintain privacy [71].

Another application of 5G in cellular and IoT networks is to manage the resources within the network. Fatima et al. [72] give a comprehensive survey on management and allocation of resources using ML and DL techniques and bringing intelligence to IoT networks. In V2X communication through the 5G wireless network, to reduce the increasing complexity of the network slicing, various ML approaches are used to automate the deployment of slices and network operations derived from the historical data of the vehicular network [73]. For resource mapping in 5G network slicing, a deep reinforcement learning model derived from the communal relationship between a node and link mapping (RLCO) is proposed in [44]. The RLCO algorithm proposed is based on this reward function, which results in network slice mapping reaching the global optimum. The dynamic network slicing or slice configuration in WiFi networks can be achieved by applying DRL approaches and can achieve promising results in highly dynamic and complex environments without expert knowledge [74].

5. Emerging Threats and Security Concerns in ML Based 5G Network Slicing

This section discusses the existing solutions on 5G, the services of 5G security, the network slicing concept, its applications, and its security concerns. The enhanced fifth generation of mobile network will bring considerable modifications in mobile technologies and communication. It advances the fields of Internet of Things (IoT), Augmented Reality (AR), and machine to machine communication such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X). The 5G network provides features such as scalability, availability, reliability, and mobility and fulfills security dimensions such as authentication, authorization, data integrity, confidentiality, availability, access control, and privacy needed for critical applications.

Network slicing is one of the key features of 5G. By slicing the physical network into multiple logical networks, each provides specified services depending upon the type of application scenario. According to Khan et al. [20], network slicing is a transition from network-as-an-infrastructure to network-as-a-service. According to the authors, network slicing put an end to the need for diverse necessities; they explored key factors in the recent advancements in network slicing by adapting several IoT smart applications. The authors also devised the taxonomy based on numerous parameters such as slicing resource levels, physical infrastructure, security, and many others. Foukas et al. [17] reviewed the existing works on 5G network slicing, identified challenges, and how will look in reality. The authors reviewed the state-of-the-art 5G network slicing and illustrated the architectures based on NGMN and 5G-PPP visions. Abidi et al. [46] have implemented a hybrid learning algorithm on a 5G network slicing dataset, presuming three phases, namely data collection, optimal weighted feature extraction (OWFE), and slicing classification. The author operated with GS-DHOA-NN + DBN-based network slicing to make network slicing more effective and accurate. Afaq et al. [75] proposed an M-Cord-based LTE network, in which they implemented a programmable and dynamic slicing mechanism, with end-to-end and logically separate resource connectivity, using vNSSF and OAI frameworks for network slicing with M-Cord, with a programmable handling control and data plane.

Security is always a key concern in the network. Lots of researchers are working on the improvement of security in the 5G network. Lal et al. [76] developed a secure 5G network framework which offers 5G services from the LTE advanced network platform. The authors also worked on various security-related issues relating to the implementation of cost-effective 5G network architectures. Ahmad et al. [77] presented various security challenges in the 5G network. The authors developed a secure 5G network architecture that overcomes all of the security-related challenges. To resolve IoT, SDN, NFV, and MEC related challenges, an artificial intelligence system was used in the 5G network. Park et al. [78] gave a detailed survey of various security and privacy-related threats to the 5G network. The authors presented various 5G network security parameters such as availability, authentication, data confidentiality, reliability, accessibility. The authors also discussed various technologies of 5G networks such as SDN, D2D, industry 4.0, MEC, AI and many others.

The growing digitization of industrial automation requires networks to be more efficient, resilient, high performing, secure, and simple to use [79]. Continuous improvement in the field of 5G and networking infrastructure, and the concept of virtualisation encountered in networks that use slicing, are both associated with risk. Cyber risk is one vital matter of security which needs to be preserved. Ehrlich et al. [80] introduced some cyber security solutions to future network management, with the aim to support automatic network management based on cyber security QoS description vectors. 5G enables IoT services to trigger new types of cyber risks. Radanliev et al. [81] provided an IoT cyber security framework, with a new epistemological analysis model that enables the assessment of unpredictable risk states in 5G-based IoT systems. Radanliev et al. [82] aimed to make an AI decision on low memory devices with the use of new and emerging forms of data in order to create a self-optimising and self-adapting autonomous artificial intelligence (AutoAI). The authors intended this iterative approach and its application in low memory devices to be beneficial to 5G network slicing.

AI is another weakness in a 5G network. A new security concern in 5G network slicing is adversarial machine learning attacks. The agents intend to fool the ML and DL models by injecting a sample of data which has had a disrupting factor added to it. Learning in the presence of adversaries with the aim of reducing the impact and defending against those adversarial ML attacks, eventually developing a secure environment, is known as adversarial machine learning [83]. Shi et al. [84] deals with flooding attacks on 5G RAN slicing by minimizing the rewards for real requests and reducing fake slicing requests by adversaries through randomizing the request weight distribution. Sagduyu et al. [85] focused on the implementation of adversarial machine learning in communication

systems. The authors present two scenarios: first, the impact of attacks on spectrum sharing in 5G, and secondly, the spoofing attacks by adversaries and their impacts on the DL based physical layer authentication system of the 5G user equipment which favours network slicing.

There are numerous applications of network slicing where technological advancement, and how 5G network slicing is embedded in people's daily routines, can be seen. Some of the applications are in vehicular communications, i.e., Vehicle-to-Vehicle (V2V), Vehicle-to-Everything (V2X), WiFi networks, Industry 4.0 applications, IoT-based applications, and many others. Kalor et al. [86] stated that Industry 4.0 applications are based on network slicing. The authors defined the use of cloud computing and IoT, and how these technologies are incorporated with the manufacturing process in industry. Additionally, they specified that the current SDN is unsuitable for heterogeneous industrial work at an abstract level.

Another type of network slicing application is Vehicle-to-Everything (V2X); it is an exchange of information between vehicles and infrastructure or other vehicles (V2I or V2V). Khan et al. [87] determines the use of 5G network slicing in vehicular communication, i.e., V2X; the authors proposed the use of network slicing combined with relaying and configured the vehicular UE functionality based on the inter-vehicular distance between the vehicles by creating two virtual slices, namely the autonomous driving slice and the infotainment slice. The authors compared their work with the RSU communication method regarding the throughput of infotainment and reliability.

WiFi networks play a pivotal role in the 5G network as everything depends upon the connectivity. Nerini et al. [88] presented two slicing algorithms based on the three features of 5G, one which runs statically to assign resources as per the slice requirement and another dynamically configures the slices. The simulation is performed over an NS3 simulator, and the results obtained statistically by KPIs outperform the current WiFi access technique.

With the emerging technology in mobile communications, 5G networks enable internet connectivity over multiple devices which are connected together. The technology behind the use of 5G is network slicing, which deals with heterogeneous networks over various devices. Slicing manages the allocation and distribution of resources over the slices. With the expansion of 5G, security concerns are brought forward, which are a matter of consideration. This section covers surveys that elaborate on different security issues and how they have been managed. Mathew [89] illustrated the concept of network slicing and how it has gained traction in 5G. The author discussed the significant challenges in slicing, such as the security and implementation of RAN. The existing solutions to these challenges are slice isolation, manual slice allocation, cryptography, and authentication.

Jain et al. [90] discussed the security issues in the 5G–IoT ecosystem, and proposed a security solution for DDoS and DoS attacks. The authors presented the 5G–IoT architecture by applying network slicing technology and implementing pattern matching IDS; IDS manages to detect intrusion in the slices and the base stations. Chemodanov et al. [91] proposed AGRA, an AI-augmented geographic routing approach for IoT-based incident-supporting applications. The authors presented an approach to advanced geographic routing using AI that relies on physical obstacle information derived from satellite imagery by applying DL. The performance of the model is shown in terms of packet delivery success ratio and path stretch.

Cunha et al. [92] explained the practical aspects such as network heterogeneity and unpredictable demands with the increased use of 5G in IoT applications. The article presented the security principles and threats associated with slicing. The authors categorized the challenges as classical and non-trivial. The classical difficulties include authentication measures, integrity measures, encryption mechanisms, etc., while the non-trivial challenges include defending against side channels and dealing with end device vulnerability. Martini et al. [93] investigated the security challenges within the ETSI NFV architectural framework with management and orchestration (MANO) security functions. The authors targeted the authorization and access control functions, and improved the performance by adopting the

continuous closed-loop usage control mechanism (UCON). The aftermath of this approach impacted the end users' experience but led to improvements in reaction time against violations of the security policies. Ni et al. [94] proposed an efficient and secure service-oriented authentication framework to support network slicing and fog computing in 5G IoT services. The authors instigated slice selection mechanisms to prevent the privacy of the users, and used session keys throughout the network to assure secure accessibility.

Porambage et al. [95] implemented a key management scheme in network slicing and a secure keying mechanism for third-party applications which are accessing the slices. The keying mechanism is designed based on multi-party computation; the proposed scheme adjusts the characteristics of the network slice concerning the required security measures and scenarios. Thantharate et al. [40] discussed the DDoS attack in network slicing, and to prevent an attack in the network, the authors modeled a deep learning-based neural network named 'Secure 5G' to identify malicious requests and transfer them to a quarantine slice. The authors framed the architecture in accordance with the three key services of the 5G network, and added an extra quarantine slice in which to deposit malicious slices. The deep learning-based 5G secure model countered the DDoS attacks by filtering malicious requests with a detection accuracy of 98%.

During the life cycle of a network slice, there are numerous attacks that threaten the network and cause distortion in the complete network or some portion of a network. Several significant studies, along with their proposed frameworks, security mechanisms, considerations, and several attacks which threaten the network, have been published and are presented in Table 5.

Table 5. The state-of-the-studies on ML based Network slicing attacks and phase wise considerations. Z1—Core Network; Z2—Fronthaul; Z3—Backhaul; Z4—Xhaul; DoS—Denial of Service; DDoS—Distributed Denial of Service; IoT—Internet of Things; MANO—Management and Orchestration; KCI—Key Compromise Impersonation; LB: Load Balancing; SD—Side Channel; RA: Resource Allocation; DT—Data Tampering. (Discussed: ✓ Never Mentioned: X Partially Mentioned: *).

Authors	Proposed framework	Security Mechanism	Security Considerations				Services					Attack Prevention			
			Z1	Z2	Z3	Z4	LB	RA	Handover	DoS	DDoS	IoT	MANO	KCI	Other Attacks
[89]	Network isolation is done through slicing, cryptography and authentication	Slice Isolation	✓	×	×	×	×	✓	×	✓	✓	×	×	×	×
[90]	5G IoT architecture using Network Slicing	Intrusion Detection System (IDS)	✓	×	×	×	✓	✓	✓	✓	✓	✓	×	×	×
[92]	Prevents security concerns at packet core using Network Slicing	Slice Isolation	✓	×	×	×	×	*	×	×	×	✓	×	×	Side Channel
[93]	Secured network slicing deployment by targeting access control and authorization	MANO Security	✓	×	×	×	×	✓	×	×	×	×	✓	×	×
[95]	Develop a secure network slicing architecture for third party application using secure key scheme	Multi party computation	✓	×	×	×	×	×	×	✓	✓	×	×	✓	Data tampering
[40]	Proposed framework Secure 5G quarantines the threats which challenge the end-end security	NN based Secure 5G network slicing model	✓	×	×	×	×	✓	*	×	✓	×	×	×	×
[94]	Efficient and secure service oriented authentication framework is proposed to support network slicing and fog computing for 5G IoT services	Privacy preserving slice selection mechanism	✓	×	×	×	×	✓	×	✓	×	✓	×	×	×
[96]	Proposed a solution which prevents Denial of Service (DoS) attack for secure network slicing	Learning assisted secure network slicing	✓	×	×	×	✓	✓	×	✓	×	✓	×	×	×
[97]	Proposed a mathematical model, which offers on-demand slice allocation with guaranteed end-end delay for 5G core network slices.	Intra and Inter Slice isolation	✓	×	×	×	×	✓	×	×	✓	*	×	×	×
[63]	To secure the main segments of the end-end 5G network, proposed a hierarchical detection scheme with reinforcement learning	Reinforcement Learning (RL)	✓	×	×	×	×	×	×	×	✓	×	×	×	Botnet attack
[98]	The potential design issues and challenges of the secure 5G mobile fronthaul architecture	Backhaul Security	✓	*	✓	*	✓	✓	✓	✓	×	×	×	×	Replay and man-in middle attack
[99]	Proposed an architectural design for 5G transfer solution which targets the integration of existing and fronthaul and backhaul technologies and interfaces.	SDN/NFV based MANO entity (XCI) and Ethernet based packet forwarding entity (XFE)	✓	✓	✓	✓	✓	*	×	×	×	×	✓	×	×
[100]	A key exchange and authentication protocol is proposed, which secures Xhaul for a moving terminal in the network. The paper targets the privacy and forward secrecy in the mobile Xhaul network.	BAN logic and AVISPA evaluations	×	✓	✓	✓	×	×	✓	✓	×	×	×	×	Replay and eavesdropping attacks
[101]	The proposed framework provides real time detection and mitigation of known attacks in 5G Network Slicing. It used P4 based switches which implemented a service function chaining protocol layer, and reduced the overhead induced on the control channel.	Frame RTP4, a P4 based framework	✓	×	×	×	✓	✓	×	×	✓	×	×	×	Zero - day attack
[102]	The capability of the IDS has been extended to identify the attacking nodes in a 5G network, despite multiple network traffic encapsulations.	IDS	✓	×	×	×	×	✓	×	×	✓	×	×	×	×
[103]	This letter introduced a new type of Distributed Slice Mobility (DSM) attack, which is caused by inter-slice mobility of the user in the 5G network. Additionally, mentioned that the damage caused by DSM is higher than DoS and yo-yo attacks, in terms of performance and economy.	Autoscaling of resources	✓	×	×	×	*	*	*	*	✓	×	×	×	Distributed Slice Mobility (DSM), yo-yo attack

The entire life cycle of a slice can be divided into four phases [104], as depicted in Figure 9, along with the respective attacks and threats associated.

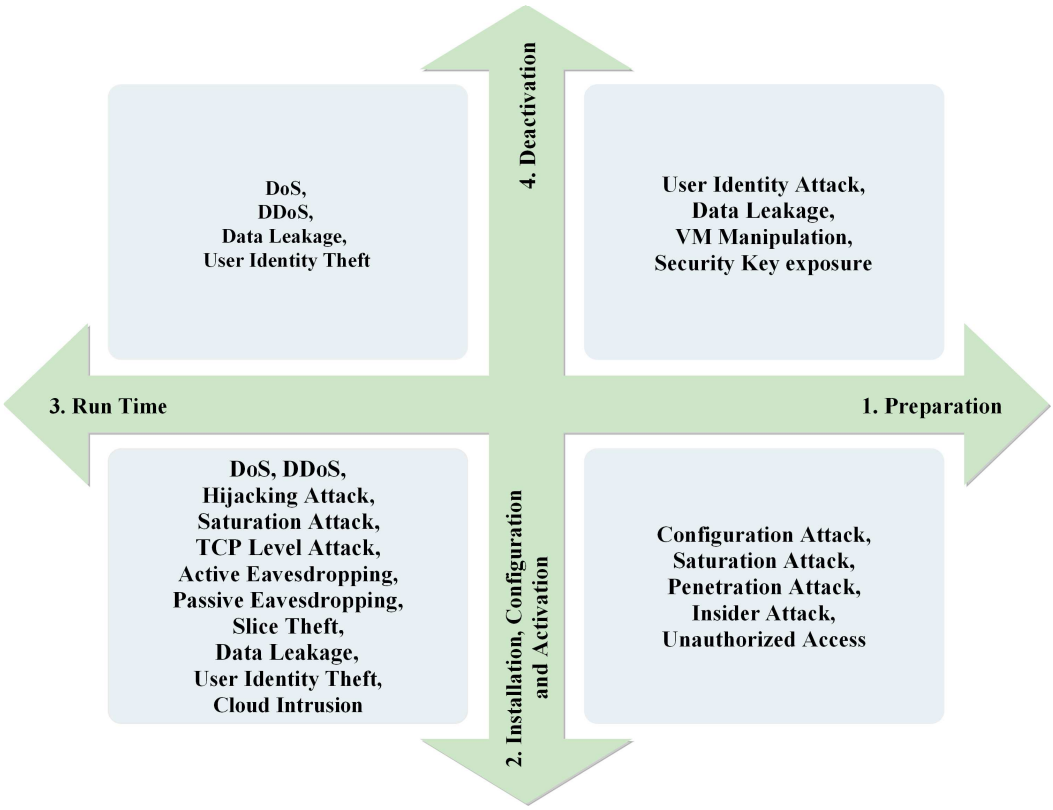

Figure 9. Life cycle of slice and the associated threats.

Preparation phase. This phase is committed to the preparation, designing, creation, and modification of the network slices. A slice is an arrangement of elements and their configuration. If there are any errors in the network slice template, they may lead to various attacks such as content exposure, data leakage, injected malware, etc. Such attacks can lead to leaked user information from the databases and access to unencrypted channels, which will cause loss of confidentiality, integrity, and authenticity of the network. Some security measures such as encryption and decryption of the slice template and real-time security analysis must be taken to prevent such attacks.

Installation, configuration, and activation phase. The second phase in the life cycle includes the installation of the slices to the network, configuration of the services as per the request, and activation of the slices, i.e., as a ready-to-use software or service. The primary threat in this phase is the creation of fake slices and re-configuration of the slices during or before the final activation. The target points of these attacks are the APIs, which can ultimately affect installation and configuration and give an activation error in a slice. Security measures must be taken to secure APIs by providing operational and accessibility rights to the authorized people and utilizing TLS or O-Auth for authentication and authorization purposes.

Run time phase. This phase signifies that the slice is in use and allows updates concerning the requirements, changes in configuration, allocation, deallocation of resources, and network functions. The targets of attacks in this phase are controllers, hypervisors, the overall cloud system, control channels, and centralized control elements. However, APIs remain the main target of attacks. The types of attacks include performance attacks, privacy breaks, and data exposure. The security measures that must be taken are authentication and integrity of the network slices to prevent fake requests, slice isolation to prevent DoS and DDoS attacks, and secure-5G modeling to prevent accessibility of unauthorized and

malicious requests. Dynamic NFV can also be used, which provides an on-demand security mechanism.

Deactivation phase. This is the last phase of the network slice's life cycle, in which the resources and network functions are relieved. The slice is no longer in use. The most common threats which can harm the network, even after the slice is decommissioned, are due to improper handling while deactivating the slice and improper usage of resources and network functions. The targets for these attacks are user information databases, cloud storage, and centralized control elements. The measures to avoid attacks in this phase are proper deallocation of the resources and network functions that are no longer in use, and deletion of sensitive data that is no longer required.

6. Network Slicing Security Solutions and Management

Figure 10 shows the taxonomic structure of NS in terms of architecture, requirement and services, security, communication, and network management. The taxonomy states the classification of the different architectural domains based on network management attributes in NS such as RAN, CN and their sub-classifications such as mMIMO, mmWAVE, SDN, and NFV, respectively. The paper has already discussed different types of standardized NS architectures in the above section, such as NGMN, ETSI, 3GPP, 5GPPP, ONF-SDN, and NFV [105].

RAN slicing is provided by the 5G network, where mobile virtual network operators share the same physical network infrastructure. According to dynamic user demands, allocation of the resources is replaced, moving from static to dynamic resources [106]. The multiple traffic services supported by the 5G NS are eMBB, mMTC, and urLLC, which are solely based on the throughput and latency requirements. The various architectures discussed above use RAN slicing for dynamic resource allocation using multiple ML and RL techniques, which are also mentioned in the above sections. CN slicing in the NS is further classified as SDN and NFV, and the SDN- and NFV-based standardized architectures have been discussed in earlier sections. E2E slicing is possible, which requires an automated management system for the creation, deletion, and updating of slices based upon the user's demands and requirements, which can be possible by providing abstract-level configuration for both the core and access network [107].

Resource provisioning for NS in a robust and efficient manner is always a challenge with the ever-growing requirements [108]. Various challenges occur while communicating between the user and the network; some tasks include dynamic resource allocation, handover, resource sharing, infrastructure sharing, and spectrum sharing. Slicing in the communication network offers different end-user services and ensures QoS within the slice. Some real-time examples are live video streaming and broadband connection while responding to medical emergencies. Infrastructure sharing is another aspect of communication management; the fundamental idea behind this concept is virtualization in the wireless network. It optimizes the cost model while increasing the overall revenue and providing scalability to the network.

Spectrum sharing in NS is the setting up of the slices in such a way as to ensure resources, which are a fixed block of a spectrum allocated to a specific network operator, can be shared with the aim of increasing the number of users who are allocated a sufficient portion of the spectrum to meet their QoS requirements. It also aims to overcome the inefficiency in the dynamic allocation of resources [109]. Handover in NS is a portable mobile communication used while moving from one base station to another without losing connection. Various ML approaches, optimization, and fuzzy logic approaches are applied to reduce the handover failure, which certainly degrades the performance of the system [110].

5G NS provides various services and fulfills the requirements of the users. Some requirements and services provided by 5G NS are eMBB, eMTC, and urLLC. eMBB stands for Enhanced Mobile Broadband, which offers a 10 to 100 GBPS peak data rate. eMBB uses macro and small cells to provide a high mobility of up to 500 Kmph. eMBB also

reduces power consumption. mMTC stands for Massive Machine Type Communication, which provides long-range connectivity with a very low data rate of up to 100 Kbps. It also provides ultra-low-cost machine to machine (M2M) communication. URLLC stands for Ultra-Reliable Low Latency Communication. It offers ultra-responsive connections among multiple devices with a latency far below 1 ms. It also offers 5 ms end-to-end latency between a mobile device and the base station. It is ultra-reliable and has 99.9999% available service, which provides medium data rates of approx. 50 Kbps to 10 Mbps. Confidentiality, authenticity, accessibility, availability, data integrity, access control are the security and privacy aspects that must be protected in 5G NS [111].

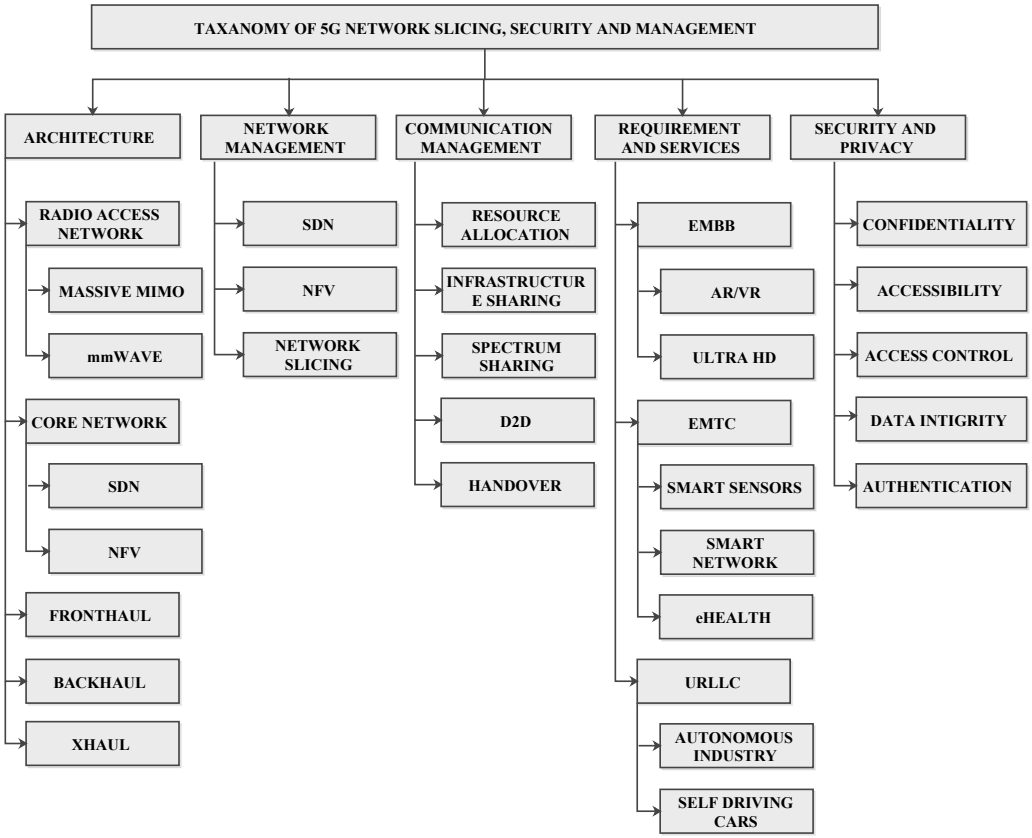

Figure 10. Taxonomy of network slicing security and management.

7. Future Directions and Research Challenges

With the growth of emerging technologies, the requirement of 5G in the market will increase, since high-speed mobile communication will be in demand to fulfill the needs of the market. With the growth of 5G networks, new challenges will also open up. By considering the various threats and challenges discussed in this paper regarding security concerns, we can see there is a need to minimize those threats in 5G network slicing. Since 5G is used in multiple sectors such as robotics, medical, automobile, agriculture, mining, media, and fashion sectors [8], as well as applications such as IoT, Industry 4.0, M2M, V2X, and many others, these issues will impact the global market in the near future, as discussed in the above sections. Therefore, security in 5G network slicing is a primary concern. This paper also discussed and illustrated the taxonomies of security measures in terms of attack prevention and machine learning algorithms at various phases of network functions. These measures must be put into action to secure 5G network slicing. Thus, following these requirements, this paper summarizes major directions to be followed in further research.

1. **AI driven 5G architecture and network slicing**—This paper discussed the various standard architectures in 5G network slicing and how they have been framed to man-

age and secure the network. The AI modulates the robustness of the 5G network [112]. The architecture should be generalized with an in-built security mechanism to handle attacks and threats [113]. A standard AI-based architecture should be framed to support flexibility, reliability, and scalability, which supports a faster data rate, improved QoS, and efficiency in the network. The security in 5G is the primary concern that must be considered.

2. **Secure authentication**—This paper discussed the various attacks and threats over the slice, which affect the user's privacy and may lead to unauthorized access. Secure mutual authentication should be incorporated to verify the authenticity and secure the application in the 5G network [113]. Therefore, a cryptographic algorithm must be applied to the channel to secure the session and keys, with real-time security analysis to prevent the network from being breached [114].
3. **Secure service migration**—Multi-access edge computing (MEC) can be applied to speed up the service migration in the network [115]. The high throughput and low latency communication with a time delay of 1 ms–10 ms is a key requirement in 5G. The connection between 5G and edge computing is empowering; 5G enables more data collection and faster processing [6], which encourages the demands of the users. Therefore, such requirements can be attained using MEC and AI techniques while supporting the properties of network slicing.
4. **Secure and continuous connectivity**—This paper discussed various attacks on the slices in a 5G network, which affect the connectivity between the end-users and the service provider. Such attacks must be minimized by adapting NN-based security measures to avoid malicious requests, unauthorized access, or intrusion within the network without affecting the network and end-user connectivity. Adversarial machine learning attacks, which affect the ML and DL models in the network, should be reduced by redesigning the models with adversarial machine learning methods as provided in [116].
5. **Fronthaul/Backhaul/Xhaul Security**—Fronthaul is an optic network link between multiple radio remote heads (RRH) and centralized baseband units (BBU) [117]. Backhaul is a bridge between RAN elements (wired network) and the mobile network, responsible for data transmission. Security in mobile backhaul is paramount. Due to continuous traffic by the 5G applicants and an increase in threats and attacks, security in mobile networks is of utmost importance [98]. Current 5G approaches employ C-RAN, but with increasing challenges and needs, it is necessary to reduce the operating cost, accelerate operation over the network, enhance the QoS, and save energy. Therefore the aim is to flexibly interconnect D-RAN and core network functions hosted over cloud network infrastructure. Xhaul architecture can enable such flexibility and reconfigure the network quickly and cost-effectively.
6. **Secure deployment**—5G has been designed by considering multiple security mechanisms with secure control over the network to provide mutual authentication, subscriber identity protection, secure service migration, secure slicing, and many other benefits. For successful deployment of 5G, the provider needs to certify all the connections and verify all the carriers' IDs, frequencies, and cell coverage in the network [118].
7. **Performance Metrics**—In 5G communication networks, several parameters are involved, all of which have an impact on the network's performance. Communication network performance can be measured in terms of the network's capacity, quality, lifetime, efficiency of routing, low latency, and high reliability. 5G networks allow lots of traffic, requiring a higher load balancing capacity to keep the networks running well. According to Choudhary et al. [98], collaboration between the RAN and backhaul will open up new possibilities for improved performance. According to recent breakthroughs in the field, the energy consumption of communication networks is based on carried traffic modeling and topology options. Throughput can be increased

through effective load balancing. Future research should concentrate on improving QoS and traffic control.

8. **Optimization**—The 5G network is made up of several sub-modules, each of which has an essential function in ensuring secure data transmissions. A network's efficiency will be harmed by channel interference and path loss. The bandwidth utilization of networks is affected by link failure and node isolation. Network slicing is a feature of 5G networks that allows for virtual network partitioning. In heterogeneous networks, time synchronization is a significant issue that affects inter-cell coordination, which are directly proportional to each other. This new idea aids in a variety of application-based network allocations. As a result, effective network slicing aids in network traffic optimization, load management, and traffic management efficiency [119].

8. Conclusions

This paper extends the understanding of the impact of network slicing over 5G. This paper explains network slicing and its layers and architectural framework by using a different standardization. The state-of-the-art comparison and road-map of the existing surveys has been discussed in addition to the timeline of the evolution of slicing. The key aspects the paper presents are the importance of security in NS and how to minimize attacks that threaten the network. Furthermore, the paper demonstrates that machine and deep learning solutions should be applied at the planning and design, construction and deployment, monitoring, fault detection, and security stages of NS, and with different application parameters and network functions. This paper gives a detailed survey of NS in 5G, machine learning-based NS and attack prevention to maintain confidentiality, authenticity, accessibility, availability, and data integrity. Finally, this paper presents a taxonomy of 5G Network Slicing, security, and management along with future directives and recommendations which anticipate a further need for analysis and evolution required in network slice security to eradicate threats and fulfill the user's requirements. This paper has shown how AI and ML can be integrated into networks in order to build self-healing and self-upgrading networks.

AI is already being integrated in networks, with the objective of minimising capital costs, improving network performance, and creating fresh revenue sources. Operators all around the globe are experiencing the advantages of AI integration in their networks. By the end of 2020, it was expected that more than half of service providers (53%) expected to have completely incorporated certain components of AI into their networks. With possibilities for leveraging machine learning and artificial intelligence to interact with 5G networks, some sectors are already scrambling to innovate with 5G. Sports, wireless virtual reality (VR), augmented reality (AR), live performances, self-driving vehicles, public safety and infrastructure, ATMs, medical equipment, remote control heavy machinery, and healthcare are just a few of the top technologies on this frontier. The upcoming industry will be surely benefited by this survey and it will help to provide a detailed study on machine learning-based approaches in 5G network slicing. This survey will also help researchers to gain knowledge and understand the facts in this field, and encourage them to further explore this field in order to benefit society and future generations.

Author Contributions: Conceptualization, A.J., R.D., G.C. and N.D.; methodology, A.J., R.D., G.C. and N.D.; validation, A.J., R.D., G.C., N.D., M.K.M. and P.L.; investigation, A.J., R.D., G.C., N.D., M.K.M. and P.L.; resources, G.C. and N.D.; Data curation, A.J., R.D. and G.C.; writing—original draft preparation, A.J., R.D. and G.C.; writing—review and editing, G.C. and N.D.; visualization, A.J., R.D., G.C., N.D., M.K.M. and P.L.; supervision, G.C., N.D., M.K.M. and P.L.; project administration, G.C. and N.D.; funding acquisition, N.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research has partially been funded by Danish Industry Foundation through project "CIDI— Cybersecure IoT in Danish Industry" (project number 2018-0197).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Li, X.; Samaka, M.; Chan, H.A.; Bhamare, D.; Gupta, L.; Guo, C.; Jain, R. Network slicing for 5G: Challenges and opportunities. *IEEE Internet Comput.* **2017**, *21*, 20–27. [CrossRef]
2. Yu, H.; Lee, H.; Jeon, H. What is 5G? Emerging 5G mobile services and network requirements. *Sustainability* **2017**, *9*, 1848. [CrossRef]
3. Werélius, G. What We Know: A Look at Current 5G Market Trends—Ericsson. 2020. Available online: https://www.ericsson.com/en/blog/2020/10/what-we-know-a-look-at-current-5g-market-trend (accessed on 17 March 2022).
4. Nokia 5G 5G in India the Journey Is about to Begin. 2021. Available online: https://telecom.economictimes.indiatimes.com/news/5g-in-india-the-journey-is-about-to-begin/81671088 (accessed on 17 March 2022).
5. 5G Companies 12 Players Are leading the Research. 2018. Available online: https://www.greyb.com/5g-companies/ (accessed on 17 March 2022).
6. Narcisi, G. These Are the 5G Trends to Watch in 2021. 2021. Available online: https://www.crn.com/news/networking/these-are-the-5g-trends-to-watch-in-2021/ (accessed on 17 March 2022).
7. Everything You Need to Know about 5G. 2020. Available online: https://www.qualcomm.com/5g/what-is-5g# (accessed on 17 March 2022).
8. Brittain, N. 5G Projects Providing a Vision for the Future. 2021. Available online: https://www.5gradar.com/features/5g-projects-that-will-blow-your-mind (accessed on 17 March 2022).
9. Zhang, H.; Liu, N.; Chu, X.; Long, K.; Aghvami, A.; Leung, V. Network Slicing Based 5G and Future Mobile Networks: Mobility. In *Resource Management, and Challenges*; IEEE Communications Magazine: 2017. Available online: https://ieeexplore.ieee.org/abstract/document/8004168 (accessed on 17 March 2023).
10. Campolo, C.; Molinaro, A.; Iera, A.; Menichella, F. 5G network slicing for vehicle-to-everything services. *IEEE Wirel. Commun.* **2017**, *24*, 38–45. [CrossRef]
11. Barakabitze, A.A.; Ahmad, A.; Mijumbi, R.; Hines, A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Comput. Netw.* **2020**, *167*, 106984. [CrossRef]
12. Kaloxylos, A. A survey and an analysis of network slicing in 5G networks. *IEEE Commun. Stand. Mag.* **2018**, *2*, 60–65. [CrossRef]
13. Chen, Q.; Liu, C.-X. A Survey of Network Slicing in 5G. In *DEStech Transactions on Computer Science and Engineering*; Elsevier: Amsterdam, The Netherlands, 2017.
14. Zhang, S. An overview of network slicing for 5G. *IEEE Wirel. Commun.* **2019**, *26*, 111–117. [CrossRef]
15. Zhang, L.; Mei, C.; Li, J.; Liang, Y.; Song, J.; Xia, X.; Zhu, X. A Survey on 5g network slicing enabling the smart grid. In Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 4–6 December 2019; pp. 911–916.
16. Ordonez-Lucena, J.; Ameigeiras, P.; Lopez, D.; Ramos-Munoz, J.J.; Lorca, J.; Folgueira, J. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Commun. Mag.* **2017**, *55*, 80–87. [CrossRef]
17. Foukas, X.; Patounas, G.; Elmokashfi, A.; Marina, M.K. Network slicing in 5G: Survey and challenges. *IEEE Commun. Mag.* **2017**, *55*, 94–100. [CrossRef]
18. Su, R.; Zhang, D.; Venkatesan, R.; Gong, Z.; Li, C.; Ding, F.; Jiang, F.; Zhu, Z. Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models. *IEEE Netw.* **2019**, *33*, 172–179. [CrossRef]
19. Richart, M.; Baliosian, J.; Serrat, J.; Gorricho, J.L. Resource slicing in virtual wireless networks: A survey. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 462–476. [CrossRef]
20. Khan, L.U.; Yaqoob, I.; Tran, N.H.; Han, Z.; Hong, C.S. Network slicing: Recent advances, taxonomy, requirements, and open research challenges. *IEEE Access* **2020**, *8*, 36009–36028. [CrossRef]
21. Rafique, W.; Qi, L.; Yaqoob, I.; Imran, M.; Rasool, R.U.; Dou, W. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1761–1804. [CrossRef]
22. Afolabi, I.; Taleb, T.; Samdanis, K.; Ksentini, A.; Flinck, H. Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2429–2453. [CrossRef]
23. 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]
24. Zhu, Y.; Ammar, M.H. Algorithms for assigning substrate network resources to virtual network components. In Proceedings of the INFOCOM, Barcelona, Spain, 23–29 April 2006; Volume 1200, pp. 1–12.
25. Shrestha, S.L.; Lee, J.; Chong, S. Virtualization and slicing of wireless mesh network. In Proceedings of the International Conference on Future Internet Technologies, Seoul, Korea, 18–20 June 2008.
26. Anadiotis, A.C.; Apostolaras, A.; Syrivelis, D.; Korakis, T.; Tassiulas, L.; Rodriguez, L.; Ott, M. A new slicing scheme for efficient use of wireless testbeds. In Proceedings of the 4th ACM International Workshop on Experimental Evaluation and Characterization, Beijing, China, 21 September 2009; pp. 83–84.

27. Sherwood, R.; Chan, M.; Covington, A.; Gibb, G.; Flajslik, M.; Handigol, N.; Huang, T.Y.; Kazemian, P.; Kobayashi, M.; Naous, J.; et al. Carving research slices out of your production networks with OpenFlow. *ACM SIGCOMM Comput. Commun. Rev.* **2010**, *40*, 129–130. [CrossRef]
28. Yiakoumis, Y.; Yap, K.K.; Katti, S.; Parulkar, G.; McKeown, N. Slicing home networks. In Proceedings of the 2nd ACM SIGCOMM Workshop on Home Networks, Toronto, ON, Canada, 15 August 2011; pp. 1–6.
29. Corin, R.D.; Gerola, M.; Riggio, R.; De Pellegrini, F.; Salvadori, E. Vertigo: Network virtualization and beyond. In Proceedings of the 2012 IEEE European Workshop on Software Defined Networking, Darmstadt, Germany, 25–26 October 2012; pp. 24–29.
30. Nikaein, N.; Schiller, E.; Favraud, R.; Katsalis, K.; Stavropoulos, D.; Alyafawi, I.; Zhao, Z.; Braun, T.; Korakis, T. Network store: Exploring slicing in future 5G networks. In Proceedings of the 10th International Workshop on Mobility in the Evolving Internet Architecture, Paris, France, 7 September 2015; pp. 8–13.
31. Shimojo, T.; Takano, Y.; Khan, A.; Kaptchouang, S.; Tamura, M.; Iwashina, S. Future mobile core network for efficient service operation. In Proceedings of the 2015 1st IEEE conference on Network Softwarization (NetSoft), London, UK, 13–17 April 2015; pp. 1–6.
32. Iwamura, M. NGMN view on 5G architecture. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–5.
33. Inam, R.; Karapantelakis, A.; Vandikas, K.; Mokrushin, L.; Feljan, A.V.; Fersman, E. Towards automated service-oriented lifecycle management for 5G networks. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–8.
34. Zhou, X.; Li, R.; Chen, T.; Zhang, H. Network slicing as a service: Enabling enterprises' own software-defined cellular networks. *IEEE Commun. Mag.* **2016**, *54*, 146–153. [CrossRef]
35. Da Silva, I.; Mildh, G.; Kaloxylos, A.; Spapis, P.; Buracchini, E.; Trogolo, A.; Zimmermann, G.; Bayer, N. Impact of network slicing on 5G Radio Access Networks. In Proceedings of the 2016 European Conference on Networks and Communications (EuCNC), Athens, Greece, 27–30 June 2016; pp. 153–157.
36. Jiang, M.; Condoluci, M.; Mahmoodi, T. Network slicing management & prioritization in 5G mobile systems. In Proceedings of the European Wireless 2016 22th European Wireless Conference, Oulu, Finland, 18–20 May 2016; pp. 1–6.
37. Hao, Y.; Tian, D.; Fortino, G.; Zhang, J.; Humar, I. Network slicing technology in a 5G wearable network. *IEEE Commun. Stand. Mag.* **2018**, *2*, 66–71. [CrossRef]
38. Li, R.; Zhao, Z.; Sun, Q.; Chih-Lin, I.; Yang, C.; Chen, X.; Zhao, M.; Zhang, H. Deep reinforcement learning for resource management in network slicing. *IEEE Access* **2018**, *6*, 74429–74441. [CrossRef]
39. Kafle, V.P.; Fukushima, Y.; Martinez-Julia, P.; Miyazawa, T. Consideration on automation of 5G network slicing with machine learning. In Proceedings of the 2018 IEEE ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K), Santa Fe, Argentina, 26–28 November 2018; pp. 1–8.
40. Thantharate, A.; Paropkari, R.; Walunj, V.; Beard, C. DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 762–767.
41. Han, B.; Schotten, H.D. Machine learning for network slicing resource management: A comprehensive survey. *arXiv* **2020**, arXiv:2001.07974.
42. Shen, X.; Gao, J.; Wu, W.; Lyu, K.; Li, M.; Zhuang, W.; Li, X.; Rao, J. AI-assisted network-slicing based next-generation wireless networks. *IEEE Open J. Veh. Technol.* **2020**, *1*, 45–66. [CrossRef]
43. Cui, Y.; Huang, X.; Wu, D.; Zheng, H. Machine Learning based Resource Allocation Strategy for Network Slicing in Vehicular Networks. In Proceedings of the 2020 IEEE/CIC International Conference on Communications in China (ICCC), Xiamen, China, 28–30 July 2020; pp. 454–459.
44. Zhao, L.; Li, L. Reinforcement learning for resource mapping in 5G network slicing. In Proceedings of the 2020 IEEE 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 869–873.
45. Lei, L.; Yuan, Y.; Vu, T.X.; Chatzinotas, S.; Minardi, M.; Montoya, J.F. Dynamic-Adaptive AI Solutions for Network Slicing Management in Satellite-Integrated B5G Systems. *IEEE Netw. Mag.* **2021**, *35*, 91–97. [CrossRef]
46. 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]
47. Ghadialy, Z. The 3G4G Blog. 2013. Available online: https://blog.3g4g.co.uk/2013/04/ (accessed on 17 March 2022).
48. Ferrús, R.; Sallent, O.; Pérez-Romero, J.; Agustí, R. Management of network slicing in 5G radio access networks: Functional framework and information models. *arXiv* **2018**, arXiv:1803.01142.
49. Choi, Y.i.; Park, N. Slice architecture for 5G core network. In Proceedings of the 2017 Ninth international conference on ubiquitous and future networks (ICUFN), Milan, Italy, 4–7 July 2017; pp. 571–575.
50. Debbabi, F.; Jmal, R.; Fourati, L.C.; Ksentini, A. Algorithmics and Modeling Aspects of Network Slicing in 5G and Beyonds Network: Survey. *IEEE Access* **2020**, *8*, 162748–162762. [CrossRef]
51. European Telecommunications Standards Institute. *Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem*; Report on Network Slicing Support with ETSI NFV Architecture Framework; ETSI: Sophia Antipolis, France, 2017.

52. Kukliński, S.; Tomaszewski, L.; Osiński, T.; Ksentini, A.; Frangoudis, P.A.; Cau, E.; Corici, M. A reference architecture for network slicing. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 217–221.
53. Duan, Q.; Ansari, N.; Toy, M. Software-defined network virtualization: An architectural framework for integrating SDN and NFV for service provisioning in future networks. *IEEE Netw.* **2016**, *30*, 10–16. [CrossRef]
54. Saboorian, T.; Xiang, A.; Thiébaut, L. *Network Slicing and 3GPP Service and Systems Aspects (SA) Standard*; IEEE Software Defined Networks, IEEE Softwarization: Piscataway, NJ, USA, 2017; Volume 7.
55. Schmit, E. The Powerful Combination of Machine Learning and 5G Networks. 2019. Available online: https://shape.att.com/blog/combination-of-machine-learning-and-5g (accessed on 17 March 2022).
56. Kelechi, A.H.; Alsharif, M.H.; Ramly, A.M.; Abdullah, N.F.; Nordin, R. The four-C framework for high capacity ultra-low latency in 5G networks: A review. *Energies* **2019**, *12*, 3449. [CrossRef]
57. Wang, H.; Wu, Y.; Min, G.; Xu, J.; Tang, P. Data-driven dynamic resource scheduling for network slicing: A deep reinforcement learning approach. *Inf. Sci.* **2019**, *498*, 106–116. [CrossRef]
58. Wang, Q.; Alcaraz-Calero, J.; Ricart-Sanchez, R.; Weiss, M.B.; Gavras, A.; Nikaein, N.; Vasilakos, X.; Giacomo, B.; Pietro, G.; Roddy, M.; et al. Enable advanced QoS-aware network slicing in 5G networks for slice-based media use cases. *IEEE Trans. Broadcast.* **2019**, *65*, 444–453. [CrossRef]
59. Gupta, R.K.; Misra, R. Machine learning-based slice allocation algorithms in 5G networks. In Proceedings of the 2019 IEEE International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 20–21 December 2019; pp. 1–4.
60. Raza, M.R.; Natalino, C.; Wosinska, L.; Monti, P. Machine learning methods for slice admission in 5g networks. In Proceedings of the 2019 IEEE 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC), Fukuoka, Japan, 7–11 July 2019; pp. 1–3.
61. Nakao, A.; Du, P. Toward in-network deep machine learning for identifying mobile applications and enabling application specific network slicing. *IEICE Trans. Commun.* **2018**, *E101-B*, 1536–1543. [CrossRef]
62. 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 IEEE 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0852–0857.
63. Sedjelmaci, H. Cooperative attacks detection based on artificial intelligence system for 5G networks. *Comput. Electr. Eng.* **2021**, *91*, 107045. [CrossRef]
64. Shi, Y.; Sagduyu, Y.E.; Erpek, T.; Gursoy, M.C. How to attack and defend 5G radio access network slicing with reinforcement learning. *arXiv* **2021**, arXiv:2101.05768.
65. Le, L.V.; Lin, B.S.P.; Tung, L.P.; Sinh, D. SDN/NFV, machine learning, and big data driven network slicing for 5G. In Proceedings of the 2018 IEEE 5G World Forum (5GWF), Santa Clara, CA, USA, 9–11 July 2018; pp. 20–25.
66. Gupta, R.K.; Choubey, A.; Jain, S.; Greeshma, R.; Misra, R. Machine Learning Based Network Slicing and Resource Allocation for Electric Vehicles (EVs). In Proceedings of the International Conference on Internet of Things and Connected Technologies, Paris, France, 14–16 December 2020; Springer: Berlin, Germany, 2020; pp. 333–347.
67. Chergui, H.; Verikoukis, C. Big data for 5G intelligent network slicing management. *IEEE Netw.* **2020**, *34*, 56–61. [CrossRef]
68. Gong, Y.; Sun, S.; Wei, Y.; Song, M. Deep Reinforcement Learning for Edge Computing Resource Allocation in Blockchain Network Slicing Broker Framework. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–6.
69. Zhou, H.; Erol-Kantarci, M.; Poor, V. Learning from Peers: Transfer Reinforcement Learning for Joint Radio and Cache Resource Allocation in 5G Network Slicing. *arXiv* **2021**, arXiv:2109.07999.
70. Shome, D.; Kudeshia, A. Deep Q-learning for 5G network slicing with diverse resource stipulations and dynamic data traffic. In Proceedings of the 2021 IEEE International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Jeju-si, Korea, 13–16 April 2021; pp. 134–139.
71. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
72. Hussain, F.; Hassan, S.A.; Hussain, R.; Hossain, E. Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1251–1275. [CrossRef]
73. Mei, J.; Wang, X.; Zheng, K. Intelligent network slicing for V2X services toward 5G. *IEEE Netw.* **2019**, *33*, 196–204. [CrossRef]
74. De Bast, S.; Torrea-Duran, R.; Chiumento, A.; Pollin, S.; Gacanin, H. Deep reinforcement learning for dynamic network slicing in IEEE 802.11 networks. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April–2 May 2019; pp. 264–269.
75. Afaq, M.; Iqbal, J.; Ahmed, T.; Islam, I.U.; Khan, M.; Khan, M.S. Towards 5G network slicing for vehicular ad hoc networks: An end-to-end approach. *Comput. Commun.* **2020**, *149*, 252–258. [CrossRef]
76. Lal, N.; Tiwari, S.M.; Khare, D.; Saxena, M. Prospects for Handling 5G Network Security: Challenges, Recommendations and Future Directions. *J. Phys. Conf. Ser.* **2021**, *1714*, 012052. [CrossRef]
77. 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]

78. Park, J.H.; Rathore, S.; Singh, S.K.; Salim, M.M.; Azzaoui, A.E.; Kim, T.W.; Pan, Y.; Park, J.H. A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions. *Hum.-Centric Comput. Inf. Sci.* **2021**, *11*, 22.
79. Wollschlaeger, M.; Sauter, T.; Jasperneite, J. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Ind. Electron. Mag.* **2017**, *11*, 17–27. [CrossRef]
80. Ehrlich, M.; Wisniewski, L.; Trsek, H.; Mahrenholz, D.; Jasperneite, J. Automatic mapping of cyber security requirements to support network slicing in software-defined networks. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–4.
81. Radanliev, P.; De Roure, D.; Burnap, P.; Santos, O. Epistemological equation for analysing uncontrollable states in complex systems: Quantifying cyber risks from the internet of things. *Rev. Socionetwork Strateg.* **2021**, *15*, 381–411. [CrossRef]
82. Radanliev, P.; De Roure, D. Review of algorithms for artificial intelligence on low memory devices. *IEEE Access* **2021**, *9*, 109986–109993. [CrossRef]
83. Adesina, D.; Hsieh, C.C.; Sagduyu, Y.E.; Qian, L. Adversarial machine learning in wireless communications using RF data: A review. *arXiv* **2020**, arXiv:2012.14392.
84. Shi, Y.; Sagduyu, Y.E. Adversarial machine learning for flooding attacks on 5G radio access network slicing. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Xiamen, China, 28–30 July 2021; pp. 1–6.
85. Sagduyu, Y.E.; Erpek, T.; Shi, Y. Adversarial machine learning for 5G communications security. In *Game Theory and Machine Learning for Cyber Security*; Cornell University: Ithaca, NY, USA, 2021; pp. 270–288.
86. Kalør, A.E.; Guillaume, R.; Nielsen, J.J.; Mueller, A.; Popovski, P. Network slicing in industry 4.0 applications: Abstraction methods and end-to-end analysis. *IEEE Trans. Ind. Inform.* **2018**, *14*, 5419–5427. [CrossRef]
87. Khan, H.; Luoto, P.; Bennis, M.; Latva-aho, M. On the application of network slicing for 5G-V2X. In Proceedings of the European Wireless 2018, 24th European Wireless Conference, Catania, Italy, 2–4 May 2018; pp. 1–6.
88. Nerini, M.; Palma, D. 5G Network Slicing for Wi-Fi Networks. *arXiv* **2021**, arXiv:2101.12644.
89. Mathew, A. Network slicing in 5G and the security concerns. In Proceedings of the 2020 IEEE Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 11–13 March 2020, pp. 75–78.
90. Jain, A.; Singh, T.; Sharma, S.K.; Prajapati, V. Implementing security in IOT ecosystem using 5G network slicing and pattern matched intrusion detection system: A simulation study. *Interdiscip. J. Inform. Knowl. Manag.* **2021**, *16*, 1–38. [CrossRef]
91. Chemodanov, D.; Esposito, F.; Sukhov, A.; Calyam, P.; Trinh, H.; Oraibi, Z. AGRA: AI-augmented geographic routing approach for IoT-based incident-supporting applications. *Future Gener. Comput. Syst.* **2019**, *92*, 1051–1065. [CrossRef]
92. Cunha, V.A.; da Silva, E.; de Carvalho, M.B.; Corujo, D.; Barraca, J.P.; Gomes, D.; Granville, L.Z.; Aguiar, R.L. Network slicing security: Challenges and directions. *Internet Technol. Lett.* **2019**, *2*, e125. [CrossRef]
93. Martini, B.; Mori, P.; Marino, F.; Saracino, A.; Lunardelli, A.; La Marra, A.; Martinelli, F.; Castoldi, P. Pushing forward security in network slicing by leveraging continuous usage control. *IEEE Commun. Mag.* **2020**, *58*, 65–71. [CrossRef]
94. Ni, J.; Lin, X.; Shen, X.S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 644–657. [CrossRef]
95. Porambage, P.; Miche, Y.; Kalliola, A.; Liyanage, M.; Ylianttila, M. Secure keying scheme for network slicing in 5G architecture. In Proceedings of the 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 28–30 October 2019; pp. 1–6.
96. Liu, Q.; Han, T.; Ansari, N. Learning-assisted secure end-to-end network slicing for cyber-physical systems. *IEEE Netw.* **2020**, *34*, 37–43. [CrossRef]
97. Sattar, D.; Matrawy, A. Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 82–90.
98. Choudhary, G.; Kim, J.; Sharma, V. Security of 5G-mobile backhaul networks: A survey. *arXiv* **2019**, arXiv:1906.11427.
99. Costa-Perez, X.; Garcia-Saavedra, A.; Li, X.; Deiss, T.; De La Oliva, A.; Di Giglio, A.; Iovanna, P.; Moored, A. 5G-crosshaul: An SDN/NFV integrated fronthaul/backhaul transport network architecture. *IEEE Wirel. Commun.* **2017**, *24*, 38–45. [CrossRef]
100. Sharma, V.; You, I.; Leu, F.Y.; Atiquzzaman, M. Secure and efficient protocol for fast handover in 5G mobile Xhaul networks. *J. Netw. Comput. Appl.* **2018**, *102*, 38–57. [CrossRef]
101. Bonfim, M.; Santos, M.; Dias, K.; Fernandes, S. A real-time attack defense framework for 5G network slicing. *Softw. Pract. Exp.* **2020**, *50*, 1228–1257. [CrossRef]
102. Mamolar, A.S.; Pervez, Z.; Calero, J.M.A.; Khattak, A.M. Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks. *Comput. Secur.* **2018**, *79*, 132–147. [CrossRef]
103. Sathi, V.N.; Murthy, C.S.R. Distributed Slice Mobility Attack: A Novel Targeted Attack Against Network Slices of 5G Networks. *IEEE Netw. Lett.* **2020**, *3*, 5–9. [CrossRef]
104. Olimid, R.F.; Nencioni, G. 5G network slicing: A security overview. *IEEE Access* **2020**, *8*, 99999–100009. [CrossRef]
105. Al-Makhadmeh, Z.; Tolba, A. Independent and tailored network-slicing architecture for leveraging industrial internet of things job processing. *Comput. Netw.* **2021**, *187*, 107827. [CrossRef]
106. Yang, P.; Xi, X.; Quek, T.Q.; Chen, J.; Cao, X.; Wu, D. RAN slicing for massive IoT and bursty URLLC service multiplexing: Analysis and optimization. *IEEE Internet Things J.* **2021**. [CrossRef]

107. Abbas, K.; Afaq, M.; Ahmed Khan, T.; Rafiq, A.; Song, W.C. Slicing the core network and radio access network domains through intent-based networking for 5g networks. *Electronics* **2020**, *9*, 1710. [CrossRef]
108. Luu, Q.T.; Kerboeuf, S.; Kieffer, M. Uncertainty-aware resource provisioning for network slicing. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 79–93. [CrossRef]
109. Li, X.; Jiao, K.; Jiang, F.; Wang, J.; Pan, M. A service-oriented spectrum-aware RAN-slicing trading scheme under spectrum sharing. *IEEE Internet Things J.* **2020**, *7*, 11303–11317. [CrossRef]
110. Sun, Y.; Jiang, W.; Feng, G.; Klaine, P.V.; Zhang, L.; Imran, M.A.; Liang, Y.C. Efficient handover mechanism for radio access network slicing by exploiting distributed learning. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 2620–2633. [CrossRef]
111. Dangi, R.; Lalwani, P.; Choudhary, G.; You, I.; Pau, G. Study and Investigation on 5G Technology: A Systematic Review. *Sensors* **2022**, *22*, 26. [CrossRef]
112. Abubakar, A.I.; Omeke, K.G.; Ozturk, M.; Hussain, S.; Imran, M.A. The role of artificial intelligence driven 5G networks in COVID-19 outbreak: Opportunities, challenges, and future outlook. *Front. Commun. Netw.* **2020**, *1*, 4. [CrossRef]
113. Choudhary, G.; Sharma, V. A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks. In *5G Enabled Secure Wireless Networks*; Springer: Berlin, Germany, 2019; pp. 69–102.
114. Dangi, R.; Pawar, S. An Improved Authentication and Data Security Approach Over Cloud Environment. In *Harmony Search and Nature Inspired Optimization Algorithms*; Springer: Berlin, Germany, 2019; pp. 1069–1076.
115. Addad, R.A.; Dutra, D.L.C.; Bagaa, M.; Taleb, T.; Flinck, H. Fast service migration in 5G trends and scenarios. *IEEE Netw.* **2020**, *34*, 92–98. [CrossRef]
116. Catak, F.O.; Kuzlu, M.; Catak, E.; Cali, U.; Unal, D. Security concerns on machine learning solutions for 6G networks in mmWave beam prediction. *Phys. Commun.* **2022**, *52*, 101626. [CrossRef]
117. Chitimalla, D.; Kondepu, K.; Valcarenghi, L.; Tornatore, M.; Mukherjee, B. 5G fronthaul–latency and jitter studies of CPRI over Ethernet. *J. Opt. Commun. Netw.* **2017**, *9*, 172–182. [CrossRef]
118. Ranaweera, C.; Monti, P.; Skubic, B.; Furdek, M.; Wosinska, L.; Nirmalathas, A.; Lim, C.; Wong, E. Optical X-haul options for 5G fixed wireless access: Which one to choose? In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 16–19 April 2018; pp. 1–2.
119. Dawaliby, S.; Bradai, A.; Pousset, Y. Network slicing optimization in large scale lora wide area networks. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019, pp. 72–77.