technologies

MDPI

Review

Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey

Bayron Jesit Ospina Cifuentes [1,2,*], Álvaro Suárez [3], Vanessa García Pineda [2], Ricardo Alvarado Jaimes [4,*], Alber Oswaldo Montoya Benitez [1,2,*] and Juan David Grajales Bustamante [5]

[1] Telematics Engineering Department (DIT), Universidad de Las Palmas de la Gran Canaria (ULPGC), 3507 Las Palmas de Gran Canaria, Spain

[2] Faculty of Engineering, Instituto Tecnológico Metropolitano, Medellín 050013, Colombia; vanessagarciap@itm.edu.co

[3] Architecture and Competition Group (GAC), Instituto Universitario de Cibernética, Empresas y Sociedad (IUCES), Universidad de Las Palmas de Gran Canaria (ULPGC), 3507 Las Palmas de Gran Canaria, Spain; alvaro.suarez@ulpgc.es

[4] New Technologies Group (GNET), Unidades Tecnológicas de Santander (UTS), Santander 680005, Colombia

[5] Measurement Analysis and Decision Support Laboratories, Department of Electronics and Telecommunications, Instituto Tecnologico Metropolitano, Medellín 050013, Colombia; juangrajales@itm.edu.co

[*] Correspondence: bayronospina@itm.edu.co (B.J.O.C.); ralvarado@correo.uts.edu.co (R.A.J.); albermontoya@itm.edu.co (A.O.M.B.)

Abstract: The distributed structure of traditional networks often fails to promptly and accurately provide the computational power required for artificial intelligence (AI), hindering its practical application and implementation. Consequently, this research aims to analyze the use of AI in software-defined networks (SDNs). To achieve this goal, a systematic literature review (SLR) is conducted based on the PRISMA 2020 statement. Through this review, it is found that, bottom-up, from the perspective of the data plane, control plane, and application plane of SDNs, the integration of various network planes with AI is feasible, giving rise to Intelligent Software Defined Networking (ISDN). As a primary conclusion, it was found that the application of AI-related algorithms in SDNs is extensive and faces numerous challenges. Nonetheless, these challenges are propelling the development of SDNs in a more promising direction through the adoption of novel methods and tools such as route optimization, software-defined routing, intelligent methods for network security, and AI-based traffic engineering, among others.

Keywords: software-defined network; artificial intelligence; traffic prediction; network security; intelligent networks

check for updates

Citation: Ospina Cifuentes, B.J.; Suárez, Á.; García Pineda, V.; Alvarado Jaimes, R.; Montoya Benitez, A.O.; Grajales Bustamante, J.D. Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey. *Technologies* **2024**, *12*, 99. https://doi.org/10.3390/technologies12070099

Academic Editor: Manoj Gupta

Received: 22 May 2024
Revised: 17 June 2024
Accepted: 18 June 2024
Published: 2 July 2024

1. Introduction

In recent years, the rapid advancement of smart devices, networking technology, and the exponential surge in user numbers have led to an explosive growth in global data traffic. This phenomenon has been accompanied by the convergence of services such as triple play (giving rise to n-play) [1]. To optimize the increasingly complex problem of large-scale converged traffic distribution, networks have become more and more heterogeneous. Heterogeneous network infrastructure leads to increased complexity for efficient organization, management, and optimization. To tackle the aforementioned issues without compromising the openness and transparency of the forwarding plane, enhancing network management, and improving the intelligence of methods, researchers [1] proposed the concept of a knowledge plane (KP), which introduces automation, recommendations, AI, and machine learning (ML) through the application of cognitive technology to achieve the separation of algorithms, strategies, objectives, and the representation of innovative models.

However, the distributed characteristics of traditional network systems hinder integral network control, leading SDNs to be considered as reducing its size and complexity [2] to compensate for the tight coupling and insufficient control of the control plane and data plane of the traditional network architecture. SDNs decouple the control plane separately to achieve separation from the data plane [3]. Thus, the data plane is solely responsible for routing and forwarding, while the control plane implements forwarding and decision-making, and the application plane provides users with programmable network services. Administrators can control forwarding according to their desires, achieving universal forwarding and efficient manipulation of network data flows, thereby enhancing flexibility.

SDNs offer promising technical support for effectively detecting and managing networks. Recently, AI technology has been widely utilized in SDN network security, traffic engineering, and other domains [4]. As research delves deeper, it has been discovered that tools such as Big Data can be leveraged for related algorithms, enhancing the operational efficiency of SDNs and reducing operational costs [5]. The combination of SDNs and AI emerges as a powerful and suitable solution for processing large amounts of data. SDNs provide a flexible and adaptable infrastructure that allows for centralized and dynamic network management, while AI offers advanced capabilities for data-driven analysis and decision-making. This combination enables the maximization of big data potential by optimizing information flow and network operational efficiency [6,7].

The technical advantages of Big Data in network planning and optimization are fully applicable in routing, traffic management, and controllers, among others, enabling the enhancement of SDNs' operational efficiency [8,9]. Compared to traditional network data centers, SDN-based data centers can dynamically allocate data center resources to different Big Data applications to meet the Service Level Agreements (SLAs) of these Big Data applications, thus achieving better performance [10]. Therefore, the proposition of AI technology is grounded in the backdrop of Big Data, and the successful combination of SDNs and Big Data ensures the success of AI-based SDNs [11].

AI leverages the global control of the SDN controller to facilitate network management and control. Integrating with the various planes of SDNs, it enables traffic prediction, enhances security optimization, and processes data intelligently. From a macro perspective, the advent of cloud computing, edge computing, and other Big Data technologies has paved the way for the application of AI in software-defined systems, enabling them to handle large-scale spatiotemporal challenges and offer advantages in complex traffic engineering and routing problems. Compared to traditional SDNs, AI-based SDNs not only have the ability to process large-scale data rapidly but, more importantly, they inherit AI characteristics and possess learning capabilities, making the network optimal [12].

In light of the above, this article will continue to discuss the challenges faced by AI-based SDNs from the following aspects: Based on the foregoing and as the main objective of this article, the analysis of AI usage in ISDNs is proposed. To achieve this, a systematic literature review methodology is developed based on the PRISMA 2020 statement. Additionally, to address the research needs, the following questions are posed:

RQ1: What are the years with the highest interest in the use of AI in ISDNs?
RQ2: What are the main research references on the use of AI in ISDNs?
RQ3: What is the thematic evolution derived from scientific production on the use of AI in ISDNs?
RQ4: What are the main thematic clusters on the use of AI in ISDNs?
RQ5: What are the growing and emerging keywords in the research field of AI usage in ISDNs?

The document is structured as follows: initially, the research methodology employed is presented. Subsequently, the results obtained from the methodology used are presented. Following this, a discussion regarding the thematic aspects and the obtained results is provided. Finally, the main conclusions derived from the results and discussion are addressed. The importance of this article is based on the main contributions of AI to SDNs, demonstrating a notable increase in research activity since 2018 and highlighting practical applications in smart cities and vehicular systems. This article fills the gap in knowledge that other investigations have not addressed yet, focusing mainly on specific technical aspects such as load balancing or security in SDNs. This research provides a broad and versatile view that includes both the development of AI models for real-time network optimization and the exploration of innovative applications in emerging sectors such as 6G wireless intelligence. Furthermore, this study emphasizes the importance of scalability and interoperability with emerging technologies, presenting a comprehensive and advanced overview in the field of AI-driven SDNs. Table 1 summarizes the main aspects addressed in this research work.

Table 1. Summary of the main aspects addressed in the study.

Topic	Description
Main focus	AI integration with SDNs for practical and innovative applications.
Increase in publications	Notable increase in research activity since 2018, with peaks in 2019 and 2021.
Practical applications	It highlights applications in smart cities and vehicle intelligence systems.
Real-time optimization	Development of AI models for real-time network optimization, dynamically adapting to changing network traffic conditions.
Interoperability	Research on the interoperability and integration of SDNs with emerging technologies such as edge computing and virtualized function networks.
Security in SDN networks	Development of high-quality datasets and advanced predictive models for threat detection and cyberattack mitigation.
Future lines of research	Scalability and efficiency of AI algorithms. Integration with 6G wireless intelligence. Security and resilience of network infrastructures.

Source: Self-elaboration based on literature review.

2. Materials and Methods

To achieve the research goal, we propose conducting a systematic review of the literature, following the guidelines outlined in the PRISMA 2020 statement. Hence, for the quantitative analysis, PRISMA guidelines are followed, focusing on metadata analysis, thus providing a holistic view of the current state of research. Thus, according to [13], the factors to be followed for PRISMA-based analysis are as follows:

a. Eligibility criteria: In the context of bibliometrics regarding the use of AI in SDNs, inclusion criteria are established based on three main aspects. First, metadata from the title and abstract are considered fundamental for record selection. Second, articles combining the concepts of "AI" and terms related to "SDN" are included. Finally, documents related to management and energy are excluded. The exclusion process consists of three phases: discarding records with incorrect indexing, excluding documents without access to full text (only for systematic literature reviews), and removing records with incomplete indexing to ensure data integrity.

b. Information source: Scopus was selected due to its relevance as a primary source of scientific information, offering extensive coverage in various disciplines. Its previous use in similar studies ensures accurate comparisons with previous research.

c. Search strategy: A specialized search equation is developed for Scopus, adapted to the inclusion criteria and characteristics of the database, ensuring the precise identification of relevant studies. Thus, the search equation is as follows:

(TITLE ("software defined network*" OR sdn OR "software-defined network*")
AND TITLE-ABS (artificial intelligence"))

d. Data management: Microsoft Excel® is employed for data extraction, storage, and processing, while VOSviewer® and Bibliometrix assist in the visualization and analysis of bibliometric indicators.
e. Selection process: An automated tool in Microsoft Excel® is used to mitigate the risk of loss or incorrect classification of relevant studies, applied by all researchers.
f. Data collection process: Microsoft Excel® is used to organize and systematize data, with participation from all authors to validate the extracted information, ensuring impartiality and objectivity.
g. Data elements: Exhaustive searches are conducted to identify all relevant articles, excluding texts with missing or unclear information to maintain study coherence and appropriateness.
h. Assessment of study bias risk: An automated tool in Microsoft Excel® is used for data collection, ensuring uniformity and coherence in the process, and all authors are involved in assessing the risk of bias.
i. Effect measures: Instead of traditional measures, the scientific landscape is analyzed through the number of publications and citations related to the topic, evaluating the temporality of keyword usage and thematic association between studies with Microsoft Excel® 365 A3, VOSviewer®1.6.18, and the R® 4.3,3 Bibliometrix tool® 4.1 via Biblioshiny.
j. Synthesis methods: Specific criteria are applied for study selection, and tables and graphical representations are used to synthesize results, employing automated bibliometric indicators with Microsoft Excel®.
k. Assessment of reporting bias: The potential influence of reporting biases in bibliometric synthesis is acknowledged, such as thesaurus biases and the exclusion of texts with incomplete indexing, requiring caution in result interpretation.
l. Certainty assessment: The certainty in the body of evidence is evaluated through inclusion and exclusion criteria, the definition of bibliometric indicators, the reporting of potential biases, and the discussion of study limitations. The recommended flowchart for methodological design is included. Additionally, Figure 1, which presents the recommended flowchart by [14] to account for the methodological design, is provided.

Regarding the systematic literature review (SLR), this methodology was employed for the qualitative component of the study, which mainly corresponded to the extraction of relevant variables and factors from the research topic. Following the research criteria and considering the required information, a search strategy in Scopus was defined to obtain the most precise results for the research. The same search equation used for the PRISMA statement was employed to address and resolve the research problem. Thus, the inclusion and exclusion criteria, as well as the SLR process, comprised the following steps according to [14]:

Study selection: After searching the Scopus database, works that were most likely to address the research problem were selected primarily based on the information they contained. For this selection, the following criteria were considered:

- Studies must be published in journals classified in quartiles Q1, Q2, and Q3 of the Scimago Journal & Country (SJC) Rank platform to ensure rigorous research and obtain quality results.
- Studies must address topics related to the use of AI in ISDNs.

- The theoretical foundations of the studies relevant to the research will be taken into account.
- A total of 140 studies obtained from Scopus were reviewed; those meeting the specified criteria for the research were selected.

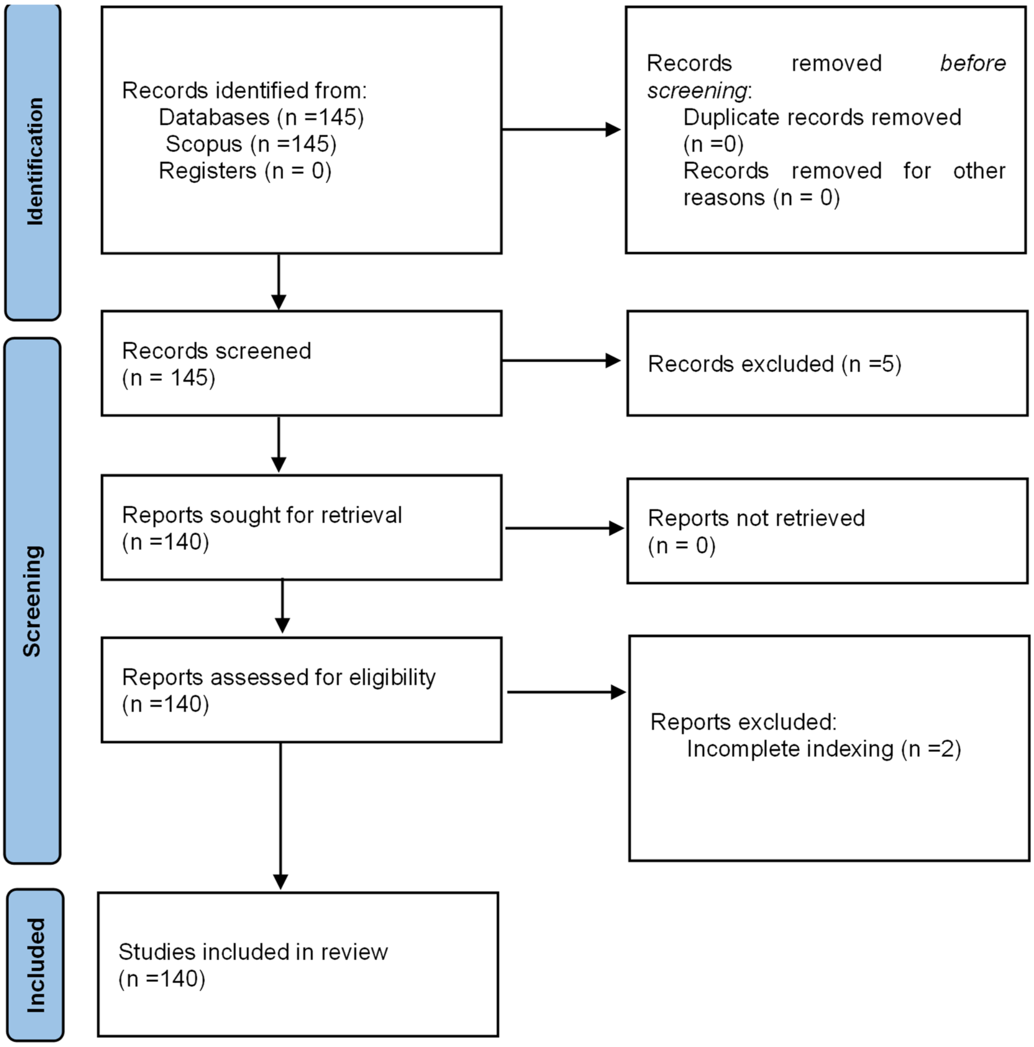
Identification
Screening
Included
Records identified from:
Databases (n =145)
Scopus (n =145)
Registers (n = 0)
Records removed *before screening*:
Duplicate records removed (n =0)
Records removed for other reasons (n = 0)
Records screened (n = 145)
Records excluded (n =5)
Reports sought for retrieval (n =140)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n =140)
Reports excluded:
Incomplete indexing (n =2)
Studies included in review (n =140)

Figure 1. PRISMA Flowchart. Self-elaboration based on Scopus.

Data collection: After searching and compiling the works, their content was analyzed, and variables to study were identified. To process the data, a database was created in Excel, considering two types of data referred to as "variables". Each variable is detailed below.

Study characterization variables: The following variables aid in recognizing and identifying each reviewed study, enabling a literature review with high-quality standards, and minimizing potential biases:

- id.
- Source.
- Journal name.
- Year of publication.
- Journal impact factor.
- SJR.
- h-index.
- Title of the study.
- Knowledge area.
- Methodological design.

- Data analysis method.

Variables related to the study's theme: These variables correspond to three groups, namely, variables related to SDNs, variables related to AI, variables related to network traffic, and finally variables related to network security.

3. Results

From the results of the PRISMA methodology (2020), indicators of quantity and quality can be identified, which gives an idea of the production and quality of research related to ISDN through the use of AI. Quantity indicators allow visualizing, among other aspects, the amount of production associated with the subject under study and, thus, the academic community's interest in this topic. Additionally, it is possible to obtain quality indicators from the results, which are obtained from the citations received by the publications in journals and authors.

3.1. Number of Publications per Year

As one of the main indicators of quantity, productivity is analyzed based on publications per year, as the ISDN theme is based on the use of ML. In this regard, Figure 2 depicts the trend of publications per year in the field of SDNs and AI, showing growing interest from approximately 2018 onwards as well as from 2021. Among the most relevant articles for the year 2019, a review article with 110 citations by [15] stands out, which presents the relationship between network applications andSDN concepts through the application of ML algorithms. Similarly, [16] describes the application of metaheuristic ML and fuzzy inference systems to the programmability of SDNs. For 2021, with 21 citations, there is a proposal focused on smart cities, where a vehicular intelligence system based on predicting the next position using VANET based on the Internet of Things (IoT) defined by software (IoTSD) is presented [17]. For the year 2023, also with 23 citations, the highest number of citations for that year is a VANET proposal based on SDN improvement as an enhancement compared to traditional VANET that may be susceptible to attacks due to its centralized structure [18]. In 2024, a proposal has been put forward focusing on the utilization of a Q-learning algorithm to optimize routing, specifically aimed at minimizing latency. This proposal adopts a direct modeling strategy to tackle the multi-path flow routing issue [19].

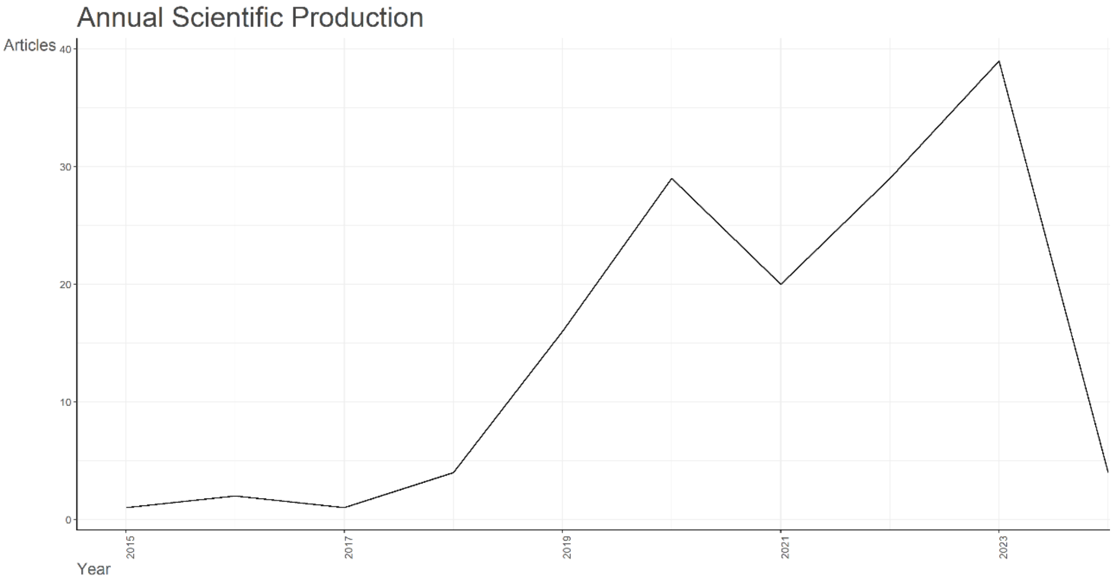

Figure 2. Articles published per year on the topic of ISDN through the use of AI. Source. Self-elaboration based on Scopus and Bibliometrix.

3.2. Number of Posts per Author

Regarding the most productive authors, Figure 3 presents the authors with the highest number of publications. Among the most productive authors are Belgaum MR., Chen J., and Musa J., with five published articles each. Among the most cited articles by these authors, one by Chen J. stands out, where he presents a software-defined framework for an integrated space-air-ground vehicular network to achieve flexible, reliable, and scalable network resource management [20]. Next, there is an article by Belgaum MR. and Musa J., presenting a systematic review of load balancing techniques in SDNs [21]. Following them are authors Alam MM. and Mazliham MS., with four publications each, among which notable articles developed in cooperation by both authors include a literature review analyzing the role of AI alongside the problems and opportunities faced by all communities in incorporating the integration of these technologies in terms of reliability and scalability [22]. Furthermore, there exists a study delving into two AI optimization methodologies, specifically Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO), employed to achieve load balancing within Software-Defined Networking (SDN) environments [23].

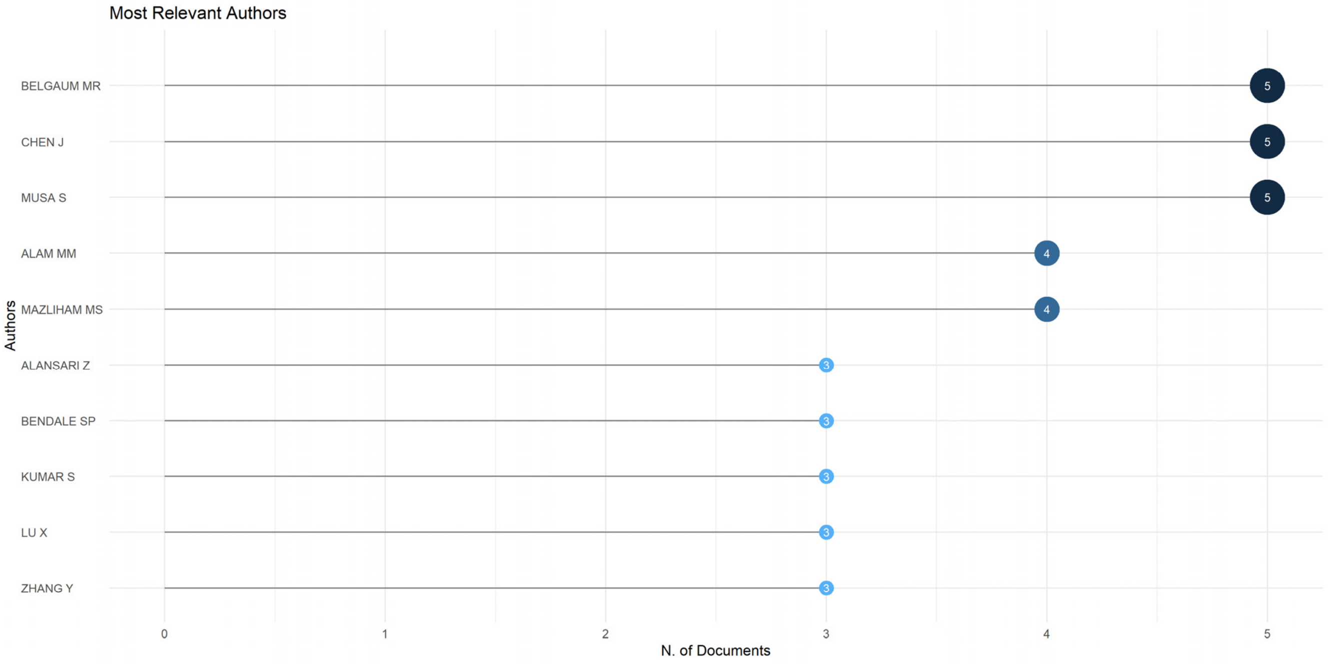

Figure 3. Articles published by authors on the topic of ISDN through the use of AI. Source. Self-elaboration based on Scopus and Bibliometrix.

On the other hand, authors Alansari Z., Bendale SP., Kumar S., Lu X., and Zhang Y. have three publications each. Among the most relevant works by these authors based on their citation count are some in collaboration with some of the aforementioned prominent authors, for example, some previously mentioned works such as [22,23]. Additionally, there is research explaining the impact of AI-enabled SDNs on infrastructure and operations, addressing trends and challenges in this knowledge area [24]. In another work by Bendale SP., with other authors, implications and applications of AI and ML concepts in SDN are reviewed, along with their future perspectives [25].

3.3. Thematic Evolution

Regarding the thematic evolution associated with the topic of ISDN through the use of AI, Figure 4 illustrates the trend and evolution of keywords over time, from 2015 to 2024. Initially, the focus of the research was on investigating and understanding AI. One of these early works was a proposal for a set of OpenFlow technologies utilizing SDN to detect network attacks, network cameras, and surveillance systems that combine wireless sensors and AI techniques [26]. Later, in 2020, advancements in AI study led to proposals such as that by [27], where the authors introduce a DDPG-EREP (Enhanced and Renewable Experience Pool) algorithm in which they suggest dynamically adjusting the capacity and sampling size of the experience pool based on the ongoing iteration number. This algorithm enables real-time updating of the experience and its application to optimize SDN routing.

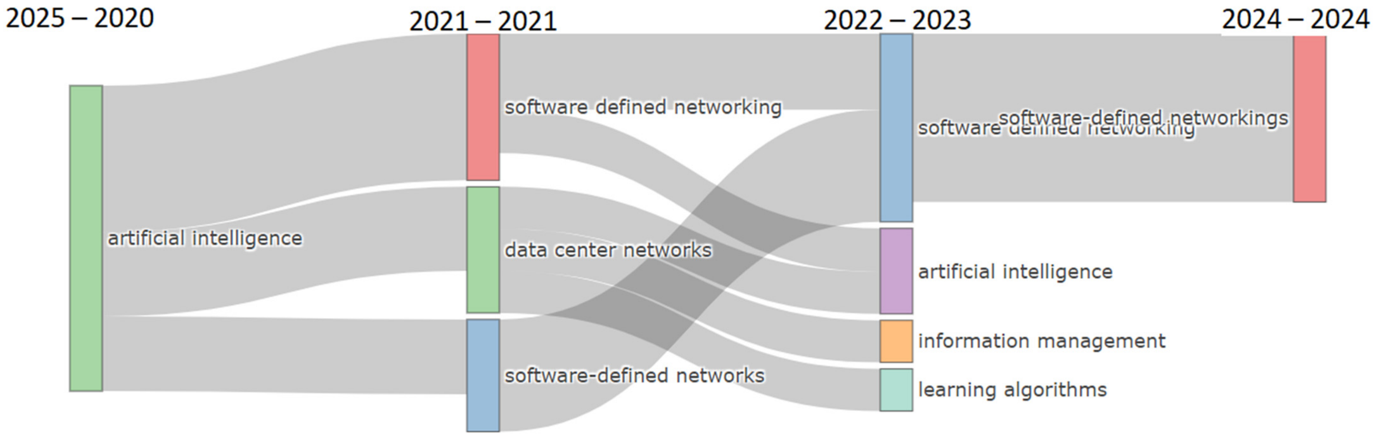

Figure 4. Trend and evolution of keywords over time in the theme of ISDN through the use of AI. Source. Self-elaboration based on Scopus and Bibliometrix.

For 2021, the most relevant and topical keywords were SDN and data center networks. A study associated with these terms introduces GDLB, a Deep Reinforcement Learning (DRL) framework devised for addressing the load balancing challenges in Software-Defined Networking (SDN) data center networks. GDLB integrates Graph Convolutional Neural Networks (GCN) with DRL techniques [28]. From 2022 to 2024, terms such as information management and learning algorithms emerge, where research focuses on the development of AI and SDN related to information management and the application of different learning algorithm techniques. A study introduces SSHS, the SDN Seamless Handover System, which integrates SDN with a machine learning classifier to oversee the network connectivity of mobile nodes. SDN centralizes control to facilitate comprehensive network management while incorporating a decision tree (DT) classifier within the RYU controller to enhance the intelligence of the SDN application. This enables the analysis and prediction of data among mobile nodes generated by the model [29]. Concerning learning algorithms, in the study conducted by [19], the authors focus on implementing a Q-learning algorithm to optimize routing, particularly aiming to minimize latency. They adopt a direct modeling approach to address the multi-path flow routing problem.

3.4. Thematic Clusters

Regarding the relationship between key terms, Figure 5 illustrates the correlation. The first cluster comprises terms such as AI, program application, SDN, network function virtualization, and 5G mobile communication systems. This cluster of words is defined by the integration of these terms in various research works. One such work presents a framework combining technologies such as SDN, network function virtualization (NFV), and ML/AI to enhance network management in OpenStack Clouds, making them more predictable, reliable, and secure [30]. The next group of terms includes keywords like SDN, network architecture, network security, denial-of-service attacks, machine learning, and learning algorithms. For this cluster primarily focused on network security, various proposals have been presented, such as that of [31], where the authors combine pervasive AI, machine learning, and quantum computing with trust management principles. They suggest an ML model inspired by quantum computing to enhance the resilience of AI-driven SDN-based network security architectures.

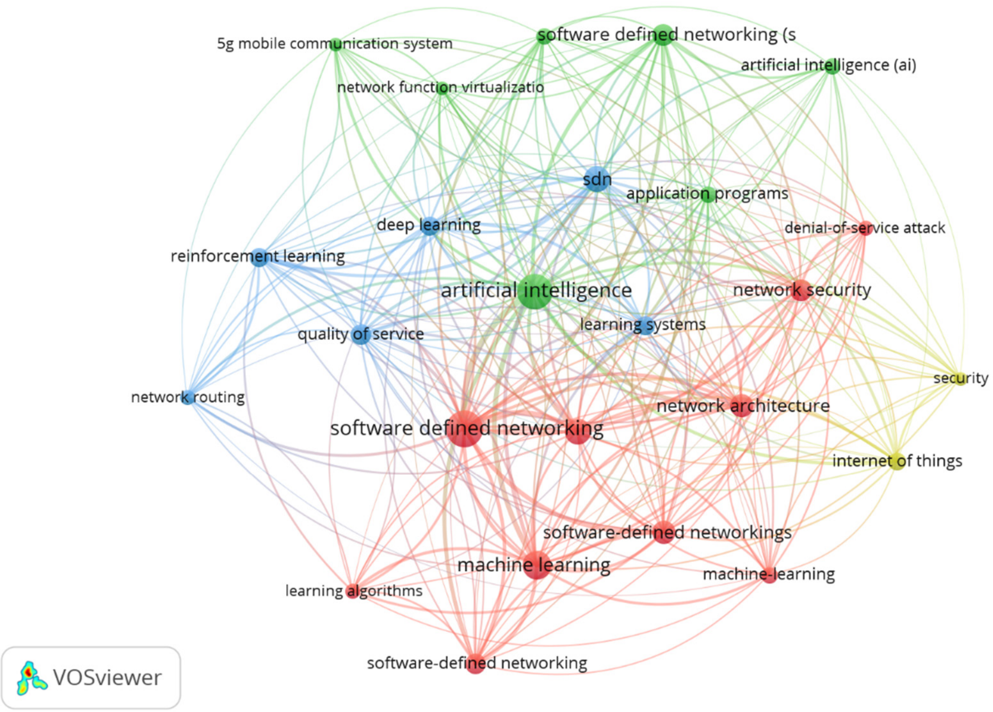

Figure 5. Correlation of keywords in the theme of ISDN through the use of AI. Source. Self-elaboration based on Scopus and VosViewer.

The following cluster comprises terms such as learning systems, SDN, deep learning, quality of service (QoS), reinforcement learning, and network routing. This cluster is based on different proposals aimed at improving network service quality and delivery, as presented in the proposal by [32]. In this study, an Intelligent SDN Routing (ISR) framework is presented, which leverages SDN technology alongside a Deep Q-Network-based network routing algorithm (TL-DQN-RA). This algorithm incorporates LSTM thresholds within SDN. TL-DQN-RA integrates Long Short-Term Memory (LSTM) into Deep Q-Network (DQN) and establishes the experience replay group threshold to expedite algorithm convergence. This allows the network to learn dynamically and adaptively modify routing strategies in response to evolving network requirements. The last group of words comprises IoT and security. This cluster emerges from the need to develop communication systems and data networks that support the IoT demand, ensuring information integrity and security. For example, in [33], they emphasize the need for internet service providers (ISPs) to better implement, configure, and automate their traffic management policies and network equipment. However, they raise concerns about the growing demand for resources from users due to aspects such as virtual reality, metaverse, IoT, and AI, among others [34].

3.5. Emerging Themes

Regarding the relevance and development of key terms, Figure 6 illustrates how terms are positioned based on their current development and relevance. In this context, the first quadrant presents terms that are more developed but currently less relevant. Here, terms such as SDN associated with sensor nodes and Wide Area Networks (WAN) can be observed. Additionally, terms like research communities, graph neural networks, and open-source software are included. The second quadrant, representing the most relevant and developed terms, corresponds to terms that are currently of greater importance, as they are the subject of ongoing research. This quadrant includes terms such as denial-of-service attacks, support vector machines, and distributed denial-of-service.

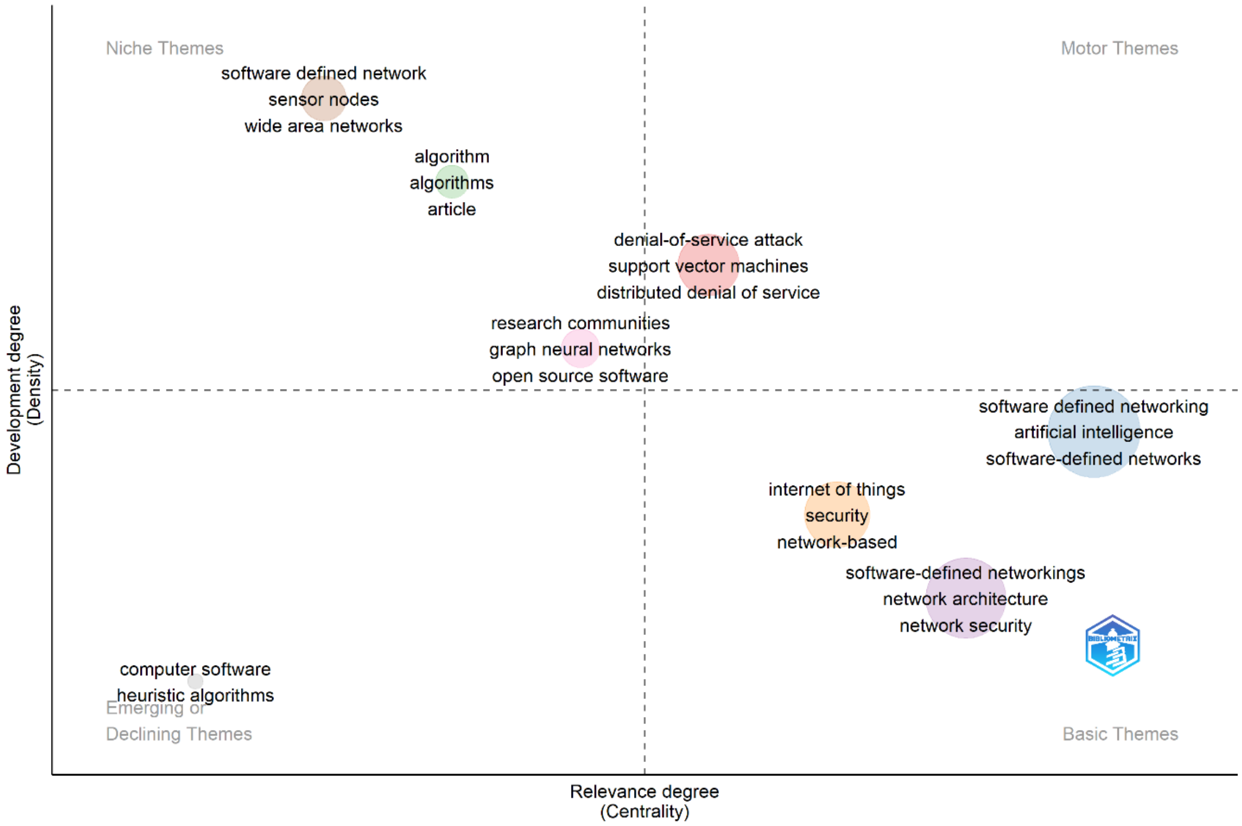

Figure 6. Relevance of keywords in the theme of ISDN through the use of AI. Source. Self-elaboration based on Scopus and Bibliometrix.

The third quadrant displays terms that are less developed and less relevant, corresponding to terms that have not been particularly prominent within the theme of interest. Here, terms like computer software and heuristic algorithms are found. In the fourth quadrant, the most relevant but less developed terms are situated. This quadrant encompasses the most recent terms, indicating emerging topics. Among the terms in this quadrant are SDN supported by AI, IoT, and network security, and SDN architecture and network security.

Thus, the aforementioned graphs illustrate the thematic evolution related to massive data management, traffic classification, route optimization, and network security. Consequently, based on these results, the analysis proceeds to explore how SDNs, especially when combined with AI, have fostered research advances in these specific fields. Therefore, a detailed examination of AI-based SDN networks is conducted, describing their application from the perspective of the three-layer architecture of SDN, comprising the data plane, control plane, and application plane.

4. Discussion

Based on the analysis of the previously obtained results, it is possible to discuss potential application scenarios and standardized definitions under SDN with AI, as well as current challenges and key SDN technologies based on AI from three aspects: route optimization, network security, and traffic engineering. Finally, addressing the future of AI-based SDN, the challenges faced, and development trends in combination with other fields.

4.1. Previous Knowledge and Related Work

4.1.1. Core Concepts Based on SDN Architecture

Below is a definition and summary presentation of some characteristics associated with SDN networks and key aspects of these networks that may be relevant to understanding their integration with AI and their relationship with different terms and topics as identified by the obtained results. Massive Data Management: SDN is considered one of the most promising solutions capable of revolutionizing the networking world through proper network management. Traffic engineering under the SDN architecture can leverage centralized SDN control through dynamic analysis, prediction, and regulation of transmission behavior, balancing network load, and maximizing network utilization to optimize network performance. However, as the network data scale continues to expand, the dimension and complexity of the data also increase. Traditional SDN urgently needs to overcome significant technical bottlenecks in data processing.

Traffic Classification: Traditional traffic classification methods primarily include port-based packet deep inspection and AI. As applications increase and ports become more dynamic, the traditional port-based traffic classification method becomes ineffective. Most packet deep inspection methods use regular expression matching to identify data packets, but there are two implementation methods: non-deterministic finite automata (NFA) and deterministic finite automata (DFA). Both have certain limitations; for example, NFAs have a smaller memory footprint but require substantial time to match. Conversely, DFAs exhibit the opposite scenario, with a higher risk of occupying excessive memory space. The current principal traffic classification methods mainly focus on using various AI methods. Although AI methods can effectively classify traffic, with the increase in application data and changes in form, there are higher requirements for the temporal and spatial complexity of algorithm training.

Route optimization within an SDN framework involves traffic routing control through the manipulation of the flow table in switches by the controller. While the controller is tasked with devising routing strategies for new flows, the majority of routing optimization techniques rely on heuristic algorithms. Heuristic algorithms bring a computational load to the controller, while AI algorithms do not require precise mathematical models of the underlying network and can quickly provide nearly optimal routing solutions after training. Therefore, AI methods are used to build stable routing solutions. Robust models and optimization methods meeting the precise and real-time routing requirements of SDN networks are future research focal points.

Network Security: In SDN networks, by applying relevant Big Data and AI algorithms, some SDN network security issues can be effectively prevented and resolved. Firstly, various effective Big Data methods are used to obtain diverse network data, and by analyzing various data, network data anomalies are detected, real-time network security confrontations are conducted, and threats are effectively prevented. Secondly, they construct ultra-high-dimensional multidimensional data models, which allow for accurate analysis of online data flows and achieve real-time attack detection and prevention using effective AI. Intelligent methods such as regression analysis and support vector machines, among others, can analyze historical network data and classify types of attacks in historical data. However, network security issues still face timeliness and non-reuse problems, and protection is a process in play, i.e., finding the next move in the chess game before the opponent is key to winning the offensive and defensive network games. Additionally, it is essential to understand the thematic evolution of communication networks, specifically data transmission networks, as well as the emergence of AI and its relationship through different methods and technologies associated with these two knowledge fields.

4.1.2. Current State of SDN

As the network continues to expand, the increase in Internet traffic and changes in user demand pose challenges. Programmable networks offer a solution to these problems.

a. SDN as an architecture

From this premise, researchers have introduced concepts such as abstraction, distributed state abstraction, and configuration abstraction [35], aiming to separate the control function from the switch in traditional networks and manage it through the control plane. A standard interface has been established to connect the data and control planes, maintaining switch identification for data exchange. The control plane provides a global view of devices across the network, integrating information and enabling unified configurations through a specific application interface. Users make configurations through this interface, facilitating the automatic deployment of forwarding devices along the path. Thus, the data forwarding path in the network is no longer tied to the data plane, resulting in an SDN architecture that separates the data plane from the control plane and features unified interface standards [36].

The benefits of SDN are diverse and have revolutionized the way networks are managed. Among them, the separation between data forwarding and control allows for greater flexibility and efficiency in network management. Furthermore, it offers robust support for software programming, facilitating network adaptation to each user's specific needs. Another key benefit is the centralized control of network status, which simplifies network management and optimizes performance. SDN technology has found application across various domains, encompassing network virtualization [37], data center networks [38], wireless LANs [39], and cloud computing [40,41]. This is achieved by separating the distinct planes present in conventional networks, namely the data plane, the control plane, and the application plane. This separation allows for more efficient and flexible network management, as reflected in the architecture shown in Figure 7.

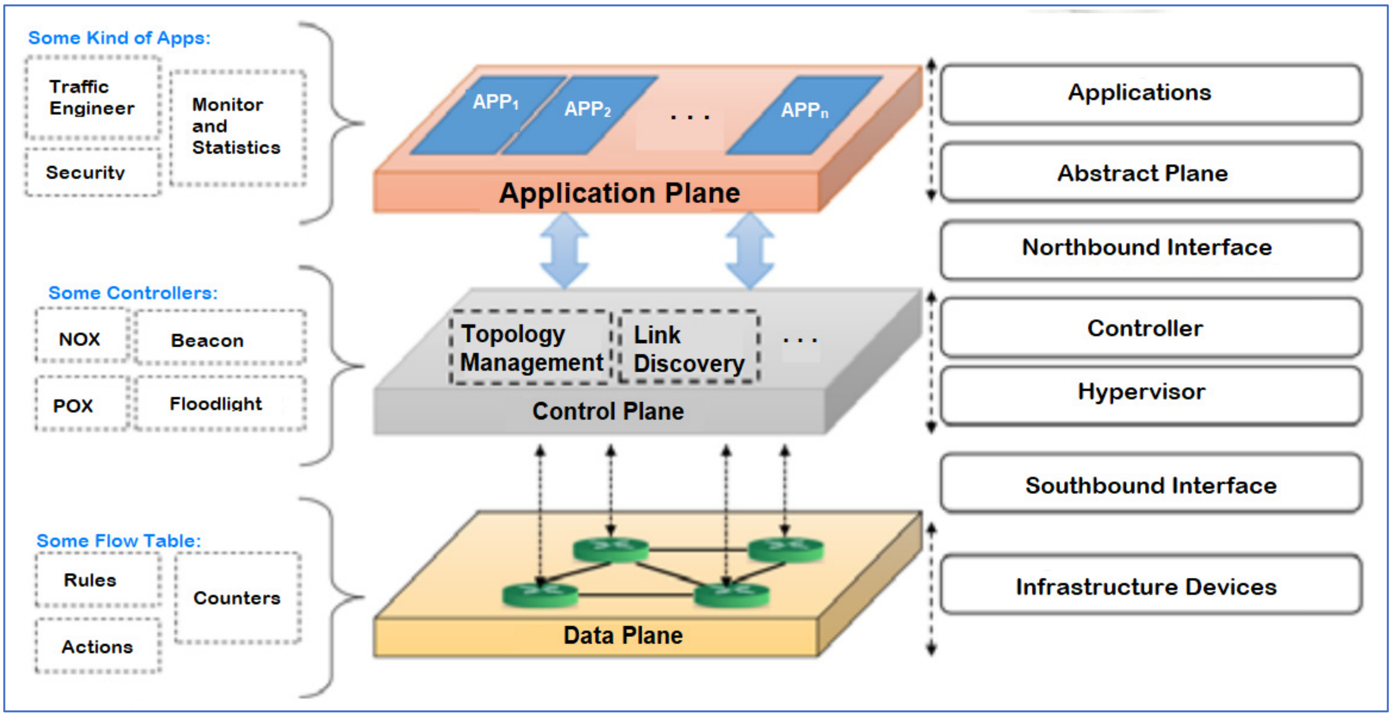

Figure 7. SDN Architecture. Source: Self-elaboration based on literature review.

The SDN architecture, represented in Figure 7, consists of three planes: application, control, and data, arranged in a descending hierarchy. In the application plane, user intentions are reflected, allowing for the development of custom applications to meet specific needs, such as network visualization and automation. Developers gather network data, such as topology and statistics, to create solutions tailored to real needs. The control plane, connected through the northbound interface, offers the possibility of custom development for users. Its main function is to manage the physical network, acquiring and maintaining vital information such as topology, thus ensuring system stability.

b. SDN as open source

SDN controllers accessible on the market are categorized into commercial and open-source options. Leading manufacturers, such as Cisco, NEC, and Brocade, offer commercial solutions. Conversely, community organizations provide open-source alternatives like Ryu, OpenDaylight, and Floodlight. These controllers play a crucial role in network operation, offering flexibility and adaptability according to user needs. Together, the SDN architecture provides an innovative approach to network management, allowing for greater customization and control over the network infrastructure.

Open-source solutions are often offered by user communities. Given their widespread adoption by individual users, the main open-source alternatives today are Ryu, OpenDaylight, and Floodlight, whose comparison is detailed in Table 2. The control plane is responsible for implementing the physical switch, which was originally hardware-based. However, with the advancement of virtualization, software switches (open vSwitch, known as OVS) have overcome the limitations of physical devices, offering integration and switching functions for virtualization and supporting distributed environments and networks based on open-source technology. At present, OVS is interoperable with standard management interfaces like NetFlow and sFlow. As for the data plane, many organizations are standardizing the southbound interface. For example, the Open Networking Foundation (ONF) has proposed the adoption of the OpenFlow protocol [42]. Likewise, the Internet Engineering Task Force's International Engineering Group has suggested the Extensible Presence and Messaging Protocol (XMPP) and other protocols defined by the IETF. The advent of OpenFlow has dismantled barriers within the SDN hardware market, enabling applications to interact with the SDN controller for exchanging data. The data plane comprises a range of fundamental devices that, via software/hardware implementation, receive directives from the higher layer through the southbound interface. These devices then process network data based on these directives and provide feedback to the higher layer through the same interface.

Table 2. Comparison between controllers.

Controller	OpenFlow Version	Language	Creator
Floodlight	1.0	Java	Big switch networks
(ODL)Open daylight	1.0, 1.3	Java	Linux foundation
ONIX	-	-	Google, Nicira
Floodlight-plus	1.3	Java	Big switch networks
Beacon	1.0.1	Java	Stanford university
Master	1.0	Java	Rich university
NOX/POX	1.0, 1.3	Python, C++	Nicira
Ryu	1.0, 1.4	Python	NTT labs

Source: Self-elaboration based on literature review.

c. SDN Simulation

Simulators play a crucial role in the research and development of networks, especially in the context of SDN. These programs have the ability to recreate network environments where data packets are sent through Ethernet ports and processed by switches and routers, allowing the simulation of network operation. This simulation is fundamental for many experiments in the field of networks, as it allows for the addition of new functions, relevant testing, and evaluation of different scenarios. Subsequently, based on the results obtained in the simulation, corresponding functions can be implemented in the real hardware environment. Table 3 provides an overview of the most commonly used simulators today, offering guidance for those seeking the right tool for their research and development needs in the field of networks.

Table 3. Comparison between Simulators.

Name	Type	OpenFlow Version	Is It Open Source?	Language	Plataform
NS-3	simulator	Pre OF 1.0 and version of OF-SID that support MPLS	Yes	Python, C++	GNUGPLv2
EstiNet	emulator/simulator	OF 1.3 and 1.0	Yes	-	LINUX
Mininet	simulator	OF 1.3 of the reference user switch and NOX from CPq D and Ericsson	Yes	Python	BSD open source

Source: Self-elaboration based on literature review.

Starting from the above, the analysis conducted from the systematic literature review allows the classification of the variables related to SDN as shown in Table 4. This presents a detailed view of SDNs, defining an architecture that addresses complex network problems through programmable networks. The separation of functions is explained, where switch control is decoupled from the traditional network and completed through the control plane connected to the data plane by a standard interface. This architectural design provides benefits such as the segregation of forwarding and control functions, software adaptability, and centralized management of network status. These advantages find utility across diverse domains like network virtualization, data centers, and cloud computing. Additionally, the three implementation planes—application, control, and data—are described, along with the use of standard protocols like OpenFlow and simulation tools for pre-implementation testing.

Table 4. Variable Classification.

Aspect	Description
Purpose	Solve complex network problems through programmable networks.
Separation of Functions	Decouples the switch control function in the traditional network, completing it through the control plane.
Standard Interface	Connects the data plane and the control plane, maintaining only the switch identification for data exchange.
Architecture	Decouples the data plane from the control plane, with unified interface standards.
Advantages	Separation of forwarding and control, support for software programmability, centralized control of network state.
Areas of Application	Network virtualization, data center network, wireless LAN, cloud computing, among other fields.
Application Plane	Reflects user intentions and allows for the development of customized applications.
Control Plane	Manages the underlying physical network, controlling SDN controllers, which can be commercial or open-source.
Data Plane	Includes basic software/hardware-based devices that process network data according to instructions from upper layers.
Standard Protocols	OpenFlow, XMPP, and others defined by the Internet Engineering Task Force (IETF).
Network Simulators	Tools for simulating and creating SDN networks, useful for testing and experiments before implementation on real hardware.

Source: Self-elaboration based on literature review.

4.1.3. Current State of AI

Since the proposal of AI at a group meeting at Dartmouth College in 1956, its ideas have profoundly influenced human science and have been widely used in image recognition [43], autonomous driving [44], pattern recognition [45], computer vision [46], and other fields. The period between the 1940s and 1970s marked the first wave of AI, during which AI focused on solving specific problems such as game rules, knowledge expression and reasoning, and expert issues. These were based on specific tasks and adapted only to specific scenarios. A typical example is the chess computer Deep Blue developed by IBM, which uses a mixed decision-making method to calculate possible chess moves and outcomes. The supercomputer decides the final chess move based on these results. Although Deep Blue was capable of predicting four to six chess moves, its high algorithmic complexity and inability to be applied to any scenario other than chess made it difficult to process large-scale data. As the scale of data increases, traditional AI methods can no longer meet the requirements.

Humans have application requirements that are beyond specific scenarios. Hence, scholars have directed their attention towards deriving rules from observational data, culminating in the advancement of technologies like natural language processing (NLP) [47], computer vision (CV) [48], and statistical machine learning (SML) [49], among others. Subsequently, supervised learning [50], unsupervised learning [51], and semi-supervised learning [52] within the realm of machine learning have emerged as focal points in artificial intelligence (AI) research. These technologies remain the most widely used and closely integrated algorithms in the field of AI. For example, in 2009, the open-source project GraphLab launched by Carlos Guestrin from Carnegie Mellon University provided powerful features, like the Application Programming Interface (API) [53]. The advantage of GraphLab is that it includes thematic models, graph analysis algorithms, graph models, clustering algorithms, and collaborative filtering algorithms, among others. Frameworks make ML statistical models easier to apply to specific AI problems, however, they require a large amount of data to drive the statistical ML algorithms.

The proposal of deep learning (DL) algorithms not only triggered a boom in DL research and applications but also marked the entry of the third wave of AI to date [54]. DL has been widely used in voice recognition [55], image recognition [56], natural language processing [57], and other fields. For example, the deep neural network-based speech recognition system launched by Microsoft broke the existing speech recognition framework and reduced the original speech recognition error rate by 20% to 30%. In addition, there is a recent and promising AI technique called Large-Scale Language Models (LLMs). These models represent significant progress in the dynamic field of AI, demonstrating unprecedented potential in various areas such as finance, business, healthcare, and cybersecurity [57].

LLMs have enabled the development of innovative applications ranging from chatbots and virtual assistants to content creation tools and personalized recommendation systems, which are briefly discussed in [58]. Regarding integration with SDNs, this is an area under exploration. The authors of [59] have started to address some reviewing aspects focused on the new frontiers and challenges of generative AI in 6G wireless intelligence.

4.2. Research on Motivations for Each SDN Plane Based on AI

Initially, the application of AI in SDN was limited to low-complexity scenarios such as routing and security. Traditional SDN separated the control plane from the forwarding plane, where the switch received instructions from the controller through a standard interface and executed actions based on predefined rules. However, this traditional model is no longer sufficient to handle the current traffic complexity and scale, especially in the era of Big Data, where formulating precise rules based on data conditions is challenging. Therefore, researchers are focused on enhancing intelligence and scalability in routing, security, and SDN architecture [60]. The application of AI in the three planes—data, control, and application—is being investigated and analyzed to understand their advantages and disadvantages. This demonstrates that AI can be integrated into all aspects of SDN, yielding beneficial results for the evolution and improvement of this technology.

4.2.1. Data Plane

Research related to the data plane addresses two main aspects: switch design and the establishment of forwarding rules. In terms of switch design, the focus is on creating fast and scalable forwarding devices capable of processing data flows quickly using flexible matching rules. On the other hand, research on forwarding rules focuses on resolving emergencies, such as coherence update issues after a rule failure. This research aims to improve the efficiency and reliability of data forwarding in network environments, contributing to the continuous development and innovation of technology in this field.

Switches are categorized into hardware switches and software switches, with HP, Cisco, Huawei, H3C, and Juniper dominating the global hardware switch market. Although hardware switches have the advantage of storing and accelerating data forwarding, excessive reliance on these devices can slow down and increase the cost of network updates. This reliance can also lead to monopolization by large companies, limiting competition and innovation in the market. The transition to software switches and the migration of some services from hardware to software can reduce costs and increase network configuration flexibility, eliminating barriers imposed by hardware manufacturers' monopolies and promoting a more competitive and innovative environment in the network equipment industry.

The International Forum on Software Switches provided a precise definition of software switches as devices and systems that use program-controlled software to offer packet network-based call control functions, enabling a wider variety of data processing methods. However, this increased functionality requires managing a large amount of code and making modifications to the system core, demanding a high level of professional knowledge from developers. To address this challenge, various clustering schemes have been proposed to improve switch performance. As an illustration, Kawashima R. and colleagues [61] devised a novel packet I/O framework named Netmap. This framework facilitated the evaluation of performance among OVS, IP forwarding, Linux bridging, and DPDK vSwitch configurations when deployed alongside OVS on Netmap. This study shed light on the different available alternatives and their respective efficiency levels in data packet processing.

Investigations into data plane forwarding rules primarily concentrate on two domains: the advancement of fresh southbound interface protocols or the proposition of intelligent protocols [62]. The segregation of the SDN control plane from the data plane provides a consolidated programming interface for network administration, enhancing its adaptability. Nonetheless, this division necessitates regular message exchanges between the OpenFlow switch and the controller via the southbound interface. This continuous exchange can overload the controller, resulting in delays in data path processing and high bandwidth requirements for the channel. To address this challenge, Zheng and others [63] proposed a southbound interface technology based on traffic characteristics, which could significantly improve the efficiency and performance of the southbound interface.

Given the uneven distribution of network traffic, focusing on a wide variety of small flows can be key to eliminating redundant routes, reducing transmission delays, and optimizing the interaction of the controller's southbound interface. Given the uneven distribution of network traffic, it has been observed that focusing on a wide variety of small flows can be key to eliminating redundant routes, reducing transmission delays, and optimizing the interaction of the controller's southbound interface. Recent research, such as that by Pandey and collaborators [64], has identified similar issues in data center networks with tree topology and proposed solutions such as a network-wide power manager and related heuristic algorithms. However, these approaches, while useful to some extent, can increase the computational load on the data plane. Therefore, it is necessary to explore data plane-based algorithms that consider the growing data scale and save energy consumption by reducing computational complexity, which could lead to more intelligent control of routing and traffic in networks.

4.2.2. Control Plane

The control plane, the core of the network, is composed of the controller, which supervises the switches in a centralized manner, streamlining data forwarding and ensuring secure global management. Current research on controllers encompasses various aspects, from optimizing routing algorithms to enhancing security and efficient resource management.

a. Research focuses on distributed controllers because a single centralized control presents challenges such as the risk of a single point of failure and processing delays in large-scale networks. Distributed controllers address these limitations by decentralizing management, improving scalability, and reducing processing times between domains and switches.

b. Research on SDN controller security is vital, given its central role in the network. Although the centralization and openness of the SDN architecture provide flexibility, they also pose significant risks. Traditional protection methods rely on OpenFlow flows but lack the capability to prevent attacks based on historical data. The introduction of artificial intelligence algorithms allows for the construction of more intelligent and effective security models. These models can leverage security information contained in historical data to improve intrusion detection and prevention. Additionally, optimizing the control plane through artificial intelligence can further enhance network security, enabling a faster and more accurate response to real-time threats and contributing to the comprehensive protection of the network infrastructure.

The application of artificial intelligence in SDN networks offers numerous advantages, particularly in traffic prediction and management. The interconnection between network status and human behavior patterns allows detailed analysis of coverage, user distribution, and other aspects, facilitating precise predictions of traffic load and future congestion. For instance, Tang et al. [65] propose a traffic load prediction algorithm based on deep learning, combined with a channel allocation algorithm that intelligently resolves channel allocation in SDN-IoT networks to avoid congestion. Khairi [66] explores SDN's capability to run machine learning algorithms and solve optimization problems centrally. These studies demonstrate how artificial intelligence can significantly improve the efficiency and management capacity of SDN networks, optimizing bandwidth use, reducing network losses, and ensuring proper load balancing.

Integrating artificial intelligence technology into the control plane offers an opportunity to enhance the security of SDN networks. For example, Hussain and collaborators [67] propose defining security rules in the SDN controller and applying machine learning algorithms based on historical data to predict potential attacks and restrict attackers' access. However, current methods face challenges as they lack real-time feedback for attack evaluation, and historical data alone may not be sufficiently accurate to identify and analyze new types of attacks. Despite these challenges, applying artificial intelligence to the control plane represents a significant step towards improving security in SDN networks, offering the possibility to identify and respond more effectively to threats.

4.2.3. Application Plane

Within SDN networks, the application plane accommodates an array of applications capable of programmatically transmitting network behavior requests to the controller via the northbound interface. Studies in this realm are bifurcated into the enhancement of northbound interfaces and the advancement of SDN applications. A milestone in the evolution towards more dynamic and flexible networks was the Google B4 architecture [68], which managed inter-data center connections but has not yet effectively addressed dynamic traffic issues. Combining artificial intelligence technologies with SDN offers promising solutions to these challenges. For example, Bu S. [69] proposed a robust traffic optimization feature based on deep learning and feature selection algorithms. This method identifies and eliminates irrelevant features in traffic data, ensuring symmetry, and then applies a model generated through deep learning to optimize traffic. This integration of artificial intelligence in the application plane enables more effective addressing of challenges associated with dynamic traffic in SDN networks, improving their performance and flexibility.

However, Internet traffic presents complex nonlinear characteristics, making it difficult to select robust features for classification and ensure optimal stability for machine learning algorithms. Fatani [70] proposed an innovative method based on multifractal wave formalization to extract multifractal features from traffic flow and apply a feature selection method based on principal component analysis to obtain relevant features, eliminating irrelevant and redundant ones. Other studies [71,72] compare methods such as Bayesian networks, decision trees, and multilayer perceptrons, performing classifications based on different types of Internet traffic and content delivery traffic. Specific research evaluates the influence of training dataset size on traffic classification performance, obtaining satisfactory results for high-speed Internet traffic classification using approaches like Bayesian networks and decision trees. These investigations represent significant advances in understanding and efficiently managing Internet traffic, especially in high-speed and complex environments.

4.3. Standardization Process of AI-Based SDN

Currently, standardization organizations such as the Open Network Foundation (ONF), the European Telecommunications Standards Institute (ETSI), the Internet Engineering Task Force (IETF), and Cisco (CISCO) are committed to standardizing AI-based SDN technologies. These organizations have different approaches and define SDN standardization from various perspectives.

4.3.1. Open Network Foundation

The ONF is composed of companies such as Google, Deutsche Telekom, and Yahoo, among others. The consortium collaboratively launches research aimed at advancing the standardization and commercial deployment of SDN and OpenFlow technology. The ONF is a user-centric entity committed to fostering and embracing SDN through the development of open standards. Emphasizing an open and cooperative development approach from the standpoint of end-users, the ONF introduced the OpenFlow standard, facilitating remote programming of the forwarding plane.

The ONF task force scrutinizes the prerequisites of SDN, formulates OpenFlow guidelines tailored to satisfy the requirements of commercial deployments, and explores novel standards to broaden the advantages of SDN. The technical community is segmented into regions, councils, and groups. These regions tackle distinct SDN-related concerns and are affiliated with SDN. They engage with foremost specialists worldwide in OpenFlow standards to deliberate on concepts, frameworks, architecture, software, standards, and certification pertaining to SDN. The Board of Directors furnishes comprehensive guidance in the strategical, operational, and technical facets of the organization. The group serves to help achieve the organization's objectives and provide guidance and suggestions for specific activities. As of late 2019, the progress of the ONF's work can be seen in Table 5.

Table 5. Progress of ONF's Work on SDN.

Classification Criteria	Main	The Progress
Specifications	Responsibilities OpenFlow related standards as technical specifications release, which may include protocol definitions, information models, component functionality and related framework < documentation.	The SPTN OpenFlow protocol extension was released in June 2017; the optical transmission protocol extension protocol was released in April 2017; and the OpenFlow switch specification version 1.5.1 was released in April 2015.
Technical advice	Including defining API, data model, protocols, and all standards and technologies such as information models. The proposal is a normative document of the ONF.	The core information model was released in November 2018; the device management interface configuration file and requirements were released in October 2018; and the OpenFlow configuration and management protocol 1.1.1 was released in March 2013.
Written documents (white papers, use cases, solutions briefings, etc.)	Help further the ONF mission and open network solution development and/or deployment publications.	Released negotiable data path model and TTP signature in September 2016; ONF SON Evolution released in September 2016.

Source: Self-elaboration based on literature review.

Given that OpenFlow explicitly declares protocol headers to indicate the operations that can be processed, increasing OpenFlow protocol headers will lead to greater system complexity and reduced flexibility. To address the issues, ONF proposed the P4 concept.

P4 is a high-level language for writing protocol-independent packet processors with the following advantages: P4 programs, irrespective of the protocol, delineate the packet handling procedures for switches. Target-independent P4 is adaptable for detailing a wide spectrum of hardware, ranging from high-speed forwarding ASICs to software-based switches. P4 enables the reconfiguration of fields, granting network engineers the ability to alter the packet processing mechanisms of switches post-deployment. Therefore, some say that SDN is the future of networking, and P4 is the future of SDN.

In December 2018, ONF held the "Next-Gen SDN Track" and proposed the combination of P4 and ML [73], which can enrich the network to obtain data. For example, traditional networks can only obtain information from the access node and the delay between routes, whereas the introduction of P4INT (in-band telemetry) technology can obtain collector ID, sequence number, timestamp, switch ID, input port, output port, hop latency, and other information. By obtaining the aforementioned information, it can be understood whether the data can predict network performance through ML technology and compare P4INT prediction results. These are combined with traditional prediction results and use previous prediction results to make correct circular decisions.

4.3.2. European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI) is a prominent international non-governmental organization of public nature. Its principal mandate involves overseeing the exploration, advancement, and establishment of technical standards concerning the Internet. Functioning as a research entity, it holds considerable influence within the global internet sector. The ETSI Industry Specification Group (ISG) proposes applying AI technology to network management systems to solve future network implementation and operation issues based on the classical OODA (observe-orient-decide-act) model. Some questions allow the system to adapt to adjust network settings and manage services with open intelligent functions based on changes in parameters such as user needs, environmental conditions, and business goals, to promote intelligent decision-making capabilities under overall industry management. This process is referred to as experiential network intelligence (ENI) [74].

The purpose of ENI is to define an architecture that combines AI technology and context-aware metadata technology based on the OODA control loop model [75] to promote changes in user needs and other changes in the decisions for adjusting the services provided. The main challenges of this model include: adapting to complex automated decision-making processes controlled by humans; determining the provision of services that can meet SLAs based on environmental changes; defining the best way to visually provide and manage network services to improve network maintenance and operations; providing an experiential architecture (i.e., combined with an AI architecture) and other mechanisms to improve understanding of the environment and experience. This model has the potential to aid decision-making systems, like network management and control systems, in adapting the services and resources offered based on alterations in user requirements, environmental factors, and business objectives.

Since its establishment in February 2017, the ISG has been specifying a set of use cases, derived requirements for technology-independent common system architectures, and a differential analysis of ENI's work on situational awareness and decision-based standards. In the same year, the ISG specified the use of AI mechanisms to learn and make decisions about high-level architecture and establish work items to create one or more proof-of-concept (PoC).

4.3.3. Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is a large-scale international public non-governmental organization. Its main role involves overseeing the research, development, and establishment of technical standards associated with the Internet. It functions as a research body with a significant level of authority within the global Internet sector. In

2017, the IETF proposed a draft on AI-driven networks (IDN) [76] to clarify the scope of IDN work and explore possible standardization efforts. The draft first analyzed existing problems with current methods, such as data and structural issues. Currently, the input and output of AI algorithms can be numerical matrices or vectors, but network data is not fully formatted or regular and needs to be translated or converted before and after the algorithm. Therefore, to fully integrate network data with AI algorithms, this combination must address deficiencies in data formatting, data compilation, etc.

Another issue is that prediction and autonomous decision-making based on AI must be a rapid response process, and the entire process must avoid congestion as much as possible. If it takes too long, then there is no point in applying AI algorithms to the network. Therefore, the draft proposes a series of solutions around how to solve such a rapid response problem. Then, the draft proposes a reference framework design method, which is of great importance in the inference and ML processes. Finally, a 3-layer IDN reference model is proposed, whose architecture can cover, explain, and support most current use cases and scenarios, and possible standardization efforts are analyzed based on this model.

4.3.4. CISCO

Cisco has risen to prominence as the foremost provider of networking solutions globally, attributed to its profound comprehension of the economic model of networks and cutting-edge technology. Its purpose is to provide strategic, innovative, and high-quality technology and solutions to the global market. In October 2019, Cisco held a global online event called "Networking.Next" and released Cisco's "Global Networking Trends 2020" based on the results of the external organization's IDC survey. The report describes the trend toward establishing Cisco's digital network readiness model. From the initial manual operation island to end-to-end management and manual operation in the information age, policy automation based on controllers in each domain is now realized on the basis of SDN. On this basis, combined with other technologies such as AI, each domain meets business needs and, finally, continues to meet dynamic business needs across all domains. The report highlights that, in past business processes, SDN played a vital role in providing continuous service performance and protection for the business in terms of automation. However, in subsequent business work, network enterprises still need to continuously monitor and optimize the network.

SDN alone cannot support an increasingly dynamic and digital business model. Therefore, it is necessary to understand changing business intentions and monitor the dynamic network conditions to continuously adapt to demand. Intent-based networks capture business intent and use analytics, ML, automatic reasoning, and automation to enable the network to continuously and dynamically adapt to changing business needs while adapting to changing network loads and other environmental influences. This can mean continuously applying and guaranteeing service performance requirements and user, security, compliance, and network technology operational strategies across the network [77].

Based on the above analysis of the systematic literature review, it is possible to classify the related intelligence variables as presented in Table 6. The variables involved in each of the three SDN planes are presented below: the data plane, the control plane, and the application plane. In the data plane, aspects such as the design of switches at both hardware and software levels, the definition of forwarding rules, the development of new southbound interface protocols, and the implementation of AI technologies to improve network performance and efficiency are addressed.

Table 6. Classification of SDN Planes Based on AI.

Plane	Variables	References
Data Plane	Switch design (hardware and software)	[61]
	Forwarding rules	[62]
	Development of new southbound interface protocols	[63]
	Intelligent protocols	[62]
	Implementation of AI technologies	[64]
Control Plane	Research on distributed controllers	[65]
	Research on controller security	[65]
	Integration of AI algorithms	[66]
Application Plane	Development of northbound interfaces	[69]
	Development of SDN applications	[68]
	Implementation of AI technologies	[70–72]

Source: Self-elaboration based on the results obtained in the literature review.

In the control plane, research related to distributed controllers, controller security, and the integration of AI algorithms for network management and optimization is highlighted. Finally, in the application plane, the development of northbound interfaces for interaction with users and external systems, the creation of specific applications for SDN, and the implementation of AI technologies to improve the functionality and adaptability of the developed applications are mentioned. Together, these variables reflect the complexity and diversity of research areas within the field of SDN, encompassing everything from low-level technical aspects to practical applications and the integration of emerging technologies such as AI.

4.4. Key Technologies and Research Methods

SDN is attracting the attention of both national and international research organizations. Artificial intelligence is being applied to analyze data and optimize networks under the centralized control and management of SDN, making administration more intelligent. This section will review AI technology to solve specific problems in SDN networks, such as intelligent routing optimization, intelligent network security methods, and AI-based traffic engineering. A brief introduction to the key technologies and research methods used in applying AI to specific problems in SDN networks will be provided.

4.4.1. Intelligent Route Optimization Method

Routing is a crucial function in networks, especially in SDN, where the controller guides traffic by modifying the flow tables of switches. Inefficient routing strategies can result in data loss, load imbalance, and inadequate resource utilization. Therefore, it is vital to develop effective routing strategies. Currently, most of these strategies are based on shortest-path optimization. For SDN, routing research focuses on optimization and defining routing. This section will briefly introduce an intelligent routing optimization method that addresses both aspects. This approach involves improving existing routing strategies and developing new strategies specifically designed for SDN, leveraging the full potential of SDN to enhance the efficiency and performance of data routing.

4.4.2. Strategy Optimization

SDN emerged as a solution to problems such as network complexity, centralized management, and vendor dependence. In current SDN networks, routing algorithms are based on Dijkstra's algorithm, which seeks the shortest path for data. However, a protocol called IPRDR has been developed for medium-sized hybrid data centers, routing traffic to devices with optimal power routes, though it is not suitable for broader scenarios [78].

Chen Y. [79] proposed an efficient SDN routing based on Q-learning to prevent congestion, but it is only applicable to certain traffic patterns. For more complex situations, additional factors must be considered. Future research should address energy optimization and congestion management in SDN networks, especially in data center environments. This involves developing algorithms that can adapt to various network conditions and improve efficiency and performance in terms of energy and congestion. The application of ML techniques and consideration of more complex variables can lead to more effective solutions for routing challenges in modern SDN networks.

Sharathkumar [80] develops new routing strategies, highlighting traffic prioritization as key. The study proposes a multi-packet forwarding framework that integrates ML and SDN to prioritize and route flows according to priority and network status. However, this approach does not consider user experience or quality of service requirements when assigning multiple routes [81]. With the increase in wireless networks, traffic control becomes crucial, as traditional routing protocols do not learn from past experiences. Finogeev [82] addresses this challenge with an intelligent flow control method based on DL, using deep convolutional neural networks (DCNN) to improve the performance of wireless networks by reducing delay and packet loss. This innovative approach seeks to solve congestion problems and improve the efficiency of the wireless mesh network (WMN). The rapid expansion of wireless networks has made effective management of network traffic, including routing techniques in wireless backbone networks, a significant challenge [82].

4.4.3. Software-Defined Routing

The core infrastructure of the Internet and heterogeneous backbone networks has maintained a similar configuration over the years, with routing algorithms that, in principle, have remained quite consistent. As the network has grown in size, the core Internet data has evolved by adding more routers and links, and this growth continues. Although the advancement of software-based routing strategies has lagged behind traditional strategies, software-defined routing (SDR) offers a cost-effective and scalable platform for packet processing, known as a programmable router. Both academia and industry are exploring the use of multicore processors to perform routing tasks in parallel, thereby improving processor performance. This multicore platform has allowed SDR to incorporate AI technologies, such as DL, to manage routing paths more efficiently. This advancement has sparked the interest of researchers and professionals in the field, as evidenced by the increase in the number of studies exploring this combination of technologies [83,84].

Currently, many researchers are immersed in research on software-defined routing (SDR). Musa [85], for example, applied a supervised DL approach, using traffic data from nodes and routers as input, to build routing tables. The results showed significant improvements in the backbone network, known as routing control. However, this method does not address security concerns at the network layer. On the other hand, Hou [86] proposed a DL-based graph approach to generate distributed routing protocols. Unlike Musa's method, this approach is topology-independent, making it applicable to a wider variety of network configurations. SDR offers flexibility by programming network devices for various purposes, eliminating the need for specific third-party hardware. This approach represents a promising advancement in improving the efficiency and security of networks.

4.4.4. Smart Methods for Network Security

SDN technology relies on a centralized controller that simplifies network management, offering optimal programmability. However, this centralization exposes the network to significant security risks. Attackers can exploit the accessibility of the network center to carry out encoded attacks, compromising the overall network security. Farris [87] examined security mechanisms in SDN, addressing issues such as the development of secure controllers, the implementation of security modules for controllers, and the defense against DoS/DDoS attacks. Additionally, specific security aspects related to the northbound direction, such as the protection of interfaces and applications, were explored. The global view of the SDN controller facilitates the collection and analysis of network traffic, enabling immediate responses to detected attacks. Numerous studies have been conducted on AI-based intrusion detection in SDN networks, including DDoS attack detection. This section will provide a comprehensive review of intelligent security methods applied to networks, highlighting the importance of addressing inherent SDN vulnerabilities to ensure the integrity and protection of the network as a whole.

Intrusion detection seeks to identify abnormal accesses to ensure network security by classifying traffic into normal and attack flows. AI methods use attributes and labels to describe each flow and determine relevant techniques to detect anomalies. For instance, Alamri [88] employed ML algorithms to define security rules in SDN controllers and prevent malicious access. However, this approach only addresses specific attacks and does not cover the detection and control of suspicious traffic. Additionally, undiscovered vulnerabilities persist in SDN controllers, allowing attackers to continue posing threats. To address these concerns, Kumar [89] proposed an SDN and ML-based intrusion detection system that detects threats in real time and includes a response system. This system uses reactive routing to analyze the impact on SDN and has been evaluated using public and real-time data. A comprehensive security design can withstand various SDN vulnerabilities and defend against a range of potential attacks, emphasizing the importance of adopting proactive approaches to safeguard network integrity.

Santos et al. [90] presented ATLANTIC, an SDN-based framework for detecting, classifying, and mitigating network anomalies. The framework comprises two stages: a lightweight phase for traffic monitoring and a heavyweight phase for anomaly classification and mitigation. In the lightweight phase, the deviation of flow table entropy is computed utilizing information theory principles, while the heavyweight phase employs the same principle to determine flow table deviation. Anomalous traffic is classified using the support vector machine (SVM) algorithm, with various techniques applied for classifying anomalies based on their severity. Leveraging the gathered data, each traffic profile is individually analyzed to obstruct malicious traffic.

DDoS attacks pose a serious threat to SDN network security by attempting to overwhelm system resources with false requests from many machines, complicating the handling of legitimate requests. These attacks exhaust network, storage, and computing resources in both the data and control planes, rendering the SDN network inoperable. Therefore, detecting DDoS attacks is crucial to maintaining normal SDN network operation. AI is essential for identifying and classifying traffic as malicious or benign, thereby reducing intrusions and DDoS attacks on SDN controllers or switches [91]. Niyaz [92] developed a DL-based DDoS detection system, integrated as an application in the SDN controller, using algorithms to reduce the features derived from network packets, proposing a DDoS detection approach in SDN environments. Although these algorithms are efficient at reducing features, they cannot directly extract features from the original traffic bytes.

SDN-based DDoS traffic detection faces significant challenges in adapting to the specific requirements of applications. Chen [93] used the XGBoost classifier along with the SDN controller to improve DDoS detection; however, these requirements have not yet been fully met. For example, the traffic threshold for DDoS attack detection may vary between different applications, but current solutions do not incorporate mechanisms to adjust to these requirements and establish the corresponding restrictions. Additionally, most SDN-based DDoS traffic detection solutions use a single controller, which can create traffic bottlenecks and single points of failure in the network. Although SDN offers centralized control over a distributed network, current solutions have yet to fully leverage this potential and must address these challenges to improve the effectiveness of DDoS traffic detection in SDN environments.

4.4.5. AI-Based Traffic Engineering

Traffic engineering (TE) is essential for enhancing data network performance through analysis, prediction, and dynamic regulation of transmitted data behavior. Although much of the research in SDN has focused on developing its architecture, SDN simplifies network management, reduces operational costs, and fosters innovation. Its unique features provide great potential for TE technologies, improving traffic control and network management. The advantage of SDN-based traffic engineering lies in its real-time reaction capability and scalability to handle large traffic volumes necessary for Internet applications.

There is an urgent need to develop a new network architecture and more intelligent and efficient TE tools to address the rapid growth of cloud computing and the demands of large-scale data centers. This new architecture must be capable of classifying and managing various types of traffic from different applications quickly and effectively, thus improving resource utilization and system performance. Integrating AI technology with SDN provides a detailed network management approach, allowing operators to handle diverse services and allocate resources more effectively. By anticipating dynamic traffic changes and developing appropriate response strategies, AI-based traffic engineering achieves precise and efficient network optimization. This approach focuses on traffic classification and identification, as well as dynamic traffic scheduling optimization, with research aimed at developing more advanced and effective methods to improve network management and performance.

4.4.6. Traffic Classification

In the context of data flow in SDN-based networks, two predominant classification methods are employed. One method distinguishes between “elephant” and “mouse” traffic [94], where elephant flows represent large and continuous traffic, while mouse flows are smaller in quantity and shorter in duration. The other method classifies traffic according to quality of service (QoS) [95,96]. In data centers, although 80% of the traffic consists of mouse flows, 20% of elephant flows consume 80% of the available bandwidth. Therefore, identifying these flows is crucial for efficiently managing traffic in the data center. Although SDN offers flexible management through flow control, this detailed management can generate considerable bandwidth consumption between the data and control planes, limiting the scalability of SDN-based data centers. The “elephant and mouse phenomenon” highlights the importance of effectively detecting and redirecting elephant flows to improve traffic management in these environments.

However, to address the challenges of high bandwidth consumption and long detection times in identifying elephant flows, Liu [97] proposed the Efficient Sampling and Classification Approach (ESCA). This approach consists of two stages: first, ESCA improves sampling efficiency by estimating the arrival interval of elephant flows and using a flow filter table to eliminate redundant samples; second, it employs a new supervised classification algorithm to categorize the samples. While this reduces bandwidth consumption and processing time, it has limitations, as it does not meet the granularity requirements of SDN data centers and campus networks, and the high computational load affects the scalability of the measurement system.

The goal of QoS-based traffic classification is to identify QoS traffic classes, which becomes challenging with the massive growth of Internet applications. Instead of identifying all applications individually, it is more practical to classify traffic according to their QoS requirements. This involves dividing applications into different QoS classes based on criteria such as jitter and loss rate. Applying AI algorithms enables multidimensional analysis of key performance indicators (KPIs), the discovery of new correlations, and the prediction of QoS violations. Additionally, it facilitates handling incomplete or corrupted data through data cleansing techniques and supports a scalable architecture capable of collecting data from both the virtual and real worlds. Thus, AI algorithms can predict QoS in big data environments and uncover additional correlations between rules [98].

4.4.7. Traffic Scheduling

In modern networks, the need to continuously adapt processing strategies to maintain optimal performance is due to the high spatiotemporal variability of traffic. This is demonstrated by the inherent diversity observed in contemporary telecommunications networks across various layers and time intervals, including unforeseen fiber outages and variations in the quality of wireless channels [99]. Additionally, the rising prevalence of smartphones and tablets as the principal devices for accessing the Internet results in an escalating demand for traffic, subsequently influencing network stability. These fluctuations in traffic demand, both in time and space, indicate the necessity of adapting input conditions to maintain optimal system performance and ensure network stability.

Additionally, online network optimization (ONO) faces the challenge of maintaining stable system performance when the actual flow situation differs from the expected situation. To address this, the flow table matching strategy in SDN reflects the dynamic processing of traffic. Jing [100] analyzed packet structure and proposed a packet matching model based on F-OpenFlow fields, allowing system performance to be adjusted according to actual network conditions and ensuring optimal or stable performance in most expected flow situations.

The proposed method aims to improve the matching probability of table entries by grouping matching fields and employing metaspace search to analyze the flow table structure in the network. It uses the Dictionary Tree Analysis Model to handle dynamic fields and achieve efficient optimization. However, it does not utilize historical data, resulting in insufficient accuracy in the relationship between message locations and flow tables, limiting the improvement of the hit rate and the flow table matching speed.

4.4.8. Traffic Prediction

Network traffic exhibits self-similar, multi-scale, and highly nonlinear characteristics, which determine its predictability. For effective network management, accurate and timely data is required for both short-term tasks and long-term planning and anomaly detection. For example, during network congestion, traditional routing cannot adjust quickly, causing issues such as high latency and packet loss. Active prediction methods, such as those used for detecting DDoS attacks, can provide early warnings. Azzouni [101] proposed NeuRoute, a dynamic routing framework that addresses these needs.

In NeuRoute, Long Short-Term Memory (LSTM) is employed to estimate future traffic, while Soud [102] develops a DL model to predict traffic. This model combines regularization and hyperbolic tangent layers to address various traffic scenarios, from free flow to congestion. The DL architecture can capture nonlinear effects, such as abrupt transitions between networks. Therefore, using DL methods for traffic prediction results in smarter routing, as the model is trained with real-time traffic data.

Although AI methods can address traffic prediction, determining the best one for all cases is challenging. Prediction accuracy depends on the amount and quality of traffic data used to train the model. Generally, neural network-based algorithms tend to offer better predictive capability and robustness than conventional models. However, most current traffic prediction methods remain superficial and do not fully meet practical needs. Therefore, it is essential to systematically analyze the literature to classify traffic-related variables, as detailed in Table 7.

Table 7. Classification of Variables According to Technologies and Methods.

Variables	Technologies and Methods	Definition	References
Route Optimization	Dijkstra's Algorithm	Method for searching the shortest path in a network.	[78]
	Intelligent Energy Reduction Decision Routing Protocol	Protocol for routing traffic by optimizing energy consumption.	[79,84]
	Q-Learning-Based Efficient SDN Routing	Routing method based on reinforcement learning to avoid congestion.	[19,79]
	Routing Strategies from the Perspective of Traffic Priority	Approach that prioritizes important traffic to avoid bottlenecks.	[80]
Software-Defined Routing	Supervised DBA	Routing approaches use supervised algorithms to improve efficiency.	[50]
	Graph-Based DL	Routing method using neural networks to learn and adapt to the network.	[86,87]
Intelligent Methods for Network Security	AI-Based Intrusion Detection	Use of AI algorithms to identify and respond to network intrusions.	[88,89]
	Network Anomaly Detection and Classification	Identification of anomalous behaviors in the network to prevent attacks.	[89]
	DL-based DDoS Attack Detection	Use of DL techniques to identify and mitigate DDoS attacks.	[92,93]
AI-Based Traffic Engineering	Traffic Classification	Process of categorizing traffic into different classes or types.	[71,72,95,96]
	Traffic Scheduling	Methods for managing and directing traffic efficiently.	[100]
	Traffic Prediction	Utilization of prediction algorithms to estimate traffic behavior.	[65,101,102]

Source: Self-elaboration based on the results obtained in the literature review.

Considering the previously mentioned variable groups and the bibliometric review conducted, the research agenda for SDN can be understood as shown in Figure 8. Some terms that are losing relevance include "network routing" and "reinforcement learning", as their emergence was around 2020, they were predominantly used that year, and they lost relevance between 2022 and 2023. Subsequently, terms such as "learning systems" and "information management" emerged around 2019, peaked in relevance in 2021, and lost significance in 2022. Regarding the term "network architecture", although it emerged around 2020 and reached its peak relevance in 2022, it remains pertinent. Therefore, the research agenda can be oriented towards "ML", "application programs", and "SDN", as these terms emerged around 2022 and are still relevant.

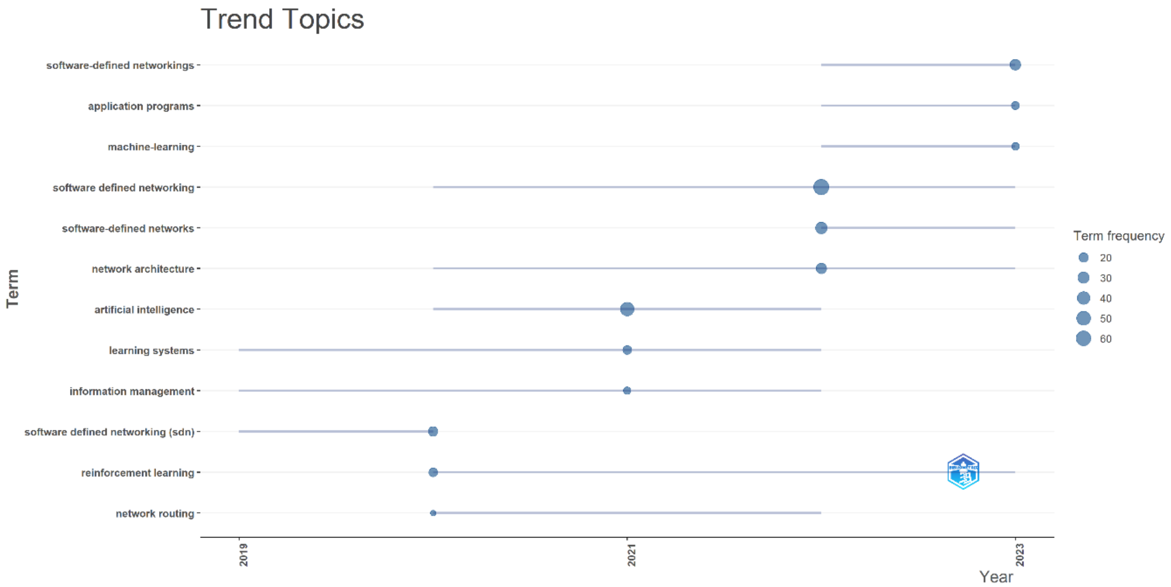

Figure 8. Relevance of Keywords in the ISDN Theme Based on the Use of AI. Source: Own elaboration based on Scopus and Bibliometrix.

4.5. Future Challenges and Network Scenarios

While AI technology can initially solve some SDN problems, challenges remain before AI can be fully integrated with SDN. These include high-quality data, inter-domain communication, scalability, and security prediction. Additionally, this section will analyze how to use AI to fully integrate SDN. The advantages of centralized SDN control combine with development trends in fields such as 5G, network function virtualization, IoT, edge computing, information center networks, and wireless networks.

4.5.1. Future Challenges

High-Quality Data

Although mature big data processing technologies and AI-based data analysis technologies exist, AI algorithms are proposed in the field of image processing rather than in the field of networks. Most algorithms cannot be transferred or used directly in network scenarios, and network data is incomplete. To meet the data format requirements of AI algorithms and apply AI to the network, network data must be translated into matrix or vector form in advance. Therefore, the prerequisite for applying AI to SDN for accurate classification prediction is that training is precise and of high quality, compensating for deficiencies in data analysis formats, data compilation, etc. Current problems are mainly divided into two aspects: on the one hand, the size of the SDN network dataset, SDN network characteristics, and the AI-based SDN network model have not yet formed. On the other hand, high-quality data can only be cleaned manually, and no public datasets are available for researchers to experiment with. Therefore, all parties need to integrate high-quality public network datasets.

a. Inter-Domain Communication

The emergence of multiple controllers aims to solve the disadvantages of increased complexity between switches and controllers caused by network-scale expansion. Research has shown that inter-domain information exchange is beneficial for improving network performance. However, data flow transmission between domains requires multiple controllers; such inter-domain design breaks the original SDN modularity. To account for the increase in multiple controllers and network complexity, traditional optimization methods are no longer sufficient to optimize the network. Although AI algorithms can be used in network optimization at all layers, analyzing the collected inter-domain information, including data link layer information, application plane information, and other information to optimize the network, such as routing mechanisms, congestion control, load balancing, etc., inter-layer optimization methods based on recursive multi-layer networks are required. Moreover, there is no mature model for inter-domain communication that facilitates future research.

On the other hand, inter-domain communication involves too many parameters, often affecting the entire system. Optimization algorithms that are truly suitable for inter-domain communication are lacking. Although many target optimization algorithms can solve the above problems with fewer parameters [103], in real situations, multi-objective optimization algorithms will cause the Pareto non-dominated problem to fail due to too many parameters, leading to the failure of the entire optimization method. Therefore, the current research aim is to establish inter-domain communication problem models and optimization methods as soon as possible.

b. Scalability

The advantages of centralized SDN control and management have increasingly attracted researchers from academia and industry to dedicate themselves to this field. While SDN offers significant opportunities for network development, it encounters numerous practical obstacles. For instance, as the network scale expands, increasing the number of controllers is necessary to share tasks and enhance the performance of the centralized controller. However, as the number of controllers increases, issues related to controller placement and dynamic control arise [104].

From this perspective, to improve the scalability of SDN networks, a multi-level RL (reinforcement learning) scheme can be considered, where the root controller acts as a high-level learning agent and the local controller as a low-level learning agent. Each lower-level learning agent acquires knowledge of directing traffic within its domain by leveraging the state information of its immediate network, thereby making optimal decisions. Conversely, the higher-level learning agent oversees inter-domain traffic management by maintaining a global perspective of the entire network. To expedite system responsiveness, the root control intermittently deploys the trained reinforcement learning (RL) model within the local controller. This trained RL model then directs the local controller to process inter-domain traffic directly. The multi-tiered RL approach not only diminishes the latency in handling commercial flows but also bolsters the scalability of the SDN network [105]. Despite the theoretical consideration of controller categorization to enhance SDN scalability using the reinforcement learning framework, there is no real-world scenario to validate the feasibility of the algorithm. Therefore, real-world situations must be considered to ensure the robustness of the entire system.

c. Security Prediction

In the previous section on network security, it was explained that the SDN controller uses AI to analyze historical data, detect network anomalies, and address network attacks. However, anomaly detection is an adversarial process. Although a mature model can be constructed using historical data to predict the next attack, malicious attackers rarely succeed in the same manner; they continuously create new attacks to evade controller detection [106]. In this context, using historical data to train an AI model is not an effective attack detection method, as it requires creating new attacks for detection. To address the aforementioned issue, two solutions can be adopted.

One solution is the Generative Adversarial Network (GAN) [107]. GAN is a method to resolve problems by predicting new attacks. GAN consists of two neural networks: a generative neural network and a discriminative neural network. The generator generates fresh data, while the discriminator assesses the genuineness of the new data by comparing it with the authentic training dataset. Both the generator and discriminator undergo joint training to enhance the realism of the newly generated data. GAN has the capability to produce potential new attack data by leveraging historical data and integrating this newly generated data with historical data to train the machine learning (ML) model. This trained ML model can detect both known and potential new attacks. Upon detecting an attack, the controller proactively adjusts the flow table in the switch to thwart network attacks and restrict communication between the control plane and the data plane.

Another method employs a prior-posterior experience model [108]. Prior experience and posterior experience can, respectively, represent historical network data information and real-time feedback information during the detection process in the model. This method retains historical information's impact on controller detection while incorporating real-time feedback information into the model to correct it. This approach can accurately and in real-time analyze network attacks to ensure the network does not suffer new attacks and cause severe consequences.

4.5.2. Applications in Different Network Scenarios

a. Fifth Generation Networks (5G)

5G networks are poised to accommodate a growing multitude of connected devices, furnish elevated user data rates, facilitate augmented mobile data traffic per unit geographical area, and diminish transmission latency and network power usage. In addition to possessing precise performance prerequisites, 5G also necessitates catering to heterogeneous services, devices, and access networks [109,110]. By separating the control and data planes, SDN significantly simplifies the network structure, reduces control signaling between network nodes, and improves load balancing, mobility management, and network control flexibility. The literature [111] proposes a centralized wireless network controller based on SDN to control multiple nodes and gateways in the core network. The purpose of the 5G network architecture based on ISDN is to meet the functional and performance requirements of a new generation of services and devices. A key feature is the flexibility required to effectively support heterogeneous service sets, including machine-type communications and IoT communications.

These applications face significant challenges regarding latency, reliability, and end-to-end availability. Challenging objectives in terms of scalability have been added. To address the challenges posed by the heterogeneous wireless environment, the complexity of network management, the growing needs of mobile communications, and the diversified service requirements in 5G mobile networks, AI technology should be used to implement smarter networks in motion [112].

b. Network Function Virtualization (NFV)

NFV enables the deployment of virtual network functions to improve performance, security, and management. Network functions are decoupled from the underlying dedicated hardware through NFV to provide flexibility in network architecture. NFVs are implemented in software running on real-world commercial devices and can be centrally controlled via an ISDN controller. Compared to traditional network functions implemented by dedicated hardware devices, NFVs have significantly lower operational and capital expenses and the potential to improve service agility. With the application of NFV, numerous related studies have become crucial services promoting network flexibility and cost-effectiveness. For instance, RL is used to dynamically create service function chains (SFC) based on resource usage to support efficient service delivery [113,114]. Combined with AI concepts, the online routing problem of SDN with NFV can be described as a linear programming model. According to this architecture, the required delay can be obtained based on resource conditions in the network, load, resource utilization, and other data to promote dynamic service delivery and optimize network resource utilization. For example, the network function allocation problem is described as a two-stage Stackelberg game, where the server acts as a network function seller and the user as a network function buyer. Wu [115] applied the RL algorithm to obtain the optimal network function allocation strategy.

c. Internet of Things (IoT)

IoT has become a global network infrastructure by connecting many different heterogeneous devices using heterogeneous communication technologies (wired/wireless).

Because of the extensive coverage and high mobility associated with these devices, a range of radio access technologies have found widespread application in the IoT. Nonetheless, the intricate nature of heterogeneous communication technologies and device infrastructure poses numerous significant challenges. For instance, as the number of devices increases, the traffic load on switches can become exceedingly burdensome, necessitating the appropriate allocation of multiple channels to links. Furthermore, heterogeneous devices have different strategies for data detection and collection, leading to the occurrence of uneven traffic bursts arriving at the switch [116,117]. To better adapt to large-scale heterogeneous IoT, ISDNs have become a novel solution for connecting distributed heterogeneous devices to centralized shared systems, termed Intelligent SDN-IoT. Within Intelligent SDN-IoT, a multitude of devices are extensively distributed across the sensing plane. The sensing data amassed by this plane is relayed and conveyed to the gateway via switches situated in the data plane. AI technology is used in combination with partially overlapping channel allocation to solve adaptive channel allocation issues and ensure the QoS of communications in wireless networks.

d. Edge Computing

Edge computing (EC) entails the deployment of computing and storage resources at the periphery of the network. Within edge computing, the term "edge" encompasses any computing and networking asset positioned between the data source and the cloud data center [118]. The integration of SDN intelligence with edge computing can yield advantages across various domains, including enhanced resolution and control, increased flexibility with fewer innovation hurdles, implementation centered around services, mobility of virtual machines, adaptability, interoperability, cost-effectiveness, and extensive coverage. Nonetheless, both Smart SDN and the current standardization of OpenFlow are not yet sufficiently developed to handle all the potential use cases and management operations outlined. As requirements change rapidly, even the relatively new standards-based realm of infrastructure as a service is also constantly evolving. Faced with increasingly complex requirements, merely deploying SDN-enabled network devices will not easily integrate SDN into existing networks. Moreover, the investment cost in hardware is very high, and therefore, smart SDN-supporting hardware cannot reach the required level in terms of functionality and deployment. Using AI technology to provide finer control granularity and abstraction granularity offers more possibilities in use cases and management.

e. Information-Centric Network (ICN)

ICNs represent an architecture designed to furnish users with content accessibility through names as opposed to establishing communication channels between hosts [119]. Integrating SDN functionalities into ICN amalgamates the network control plane with the data plane, thereby facilitating centralized programming and network control from a holistic standpoint. The amalgamated SDN-ICN framework, which combines ICN and SDN, proves advantageous in capitalizing on the data autonomy of the data plane within ICN and the centralized control afforded by the control plane in SDN for enhanced global network management. Initially, content devoid of address constraints in ICN is routed and forwarded as an autonomous entity at the network layer. Centralized scheduling facilitated by SDN can optimize the allocation of network resources [120,121].

There are numerous computing nodes in SDN-ICN. The use of AI can simultaneously learn with ICN, reducing the delay caused by ICN data processing. Therefore, due to the use of rich computing resources scattered across various SDN nodes, it can address the computation time issue during the AI model training process. Secondly, based on the unification of data collection and analysis from a global perspective, multi-scale traffic prediction can be achieved with flow-oriented characteristics for greater accuracy. Multiple switches in distributed SDN collect features of the requested target content. These features contain inherent spatiotemporal and social correlations, which DL networks can comprehend from a global view. Consequently, due to the unsupervised learning capabilities of DL networks, they can find the distribution pattern of content popularity without missing small pattern changes, thus improving prediction accuracy. Foremost, SDN-ICN holds the capability to modify the structure of the DL network. This stems from the programmability inherent in SDN and the overarching control exerted by the SDN controller over the network. Consequently, hidden layers and neurons within SDN-ICN can be readily reconfigured at each layer. Leveraging this programmable infrastructure, diverse network models can be seamlessly integrated to address computational challenges encountered within the SDN-ICN framework [122].

f. Wireless Network

A wireless network (WN) consists of many nodes and transmits through wireless channels. Unlike wired networks, wireless network channels always change with user mobility, channel fading, and interference. In dense wireless networks with mobile users and small cell sizes, channel capacity changes are more challenging to handle [123,124]. Integrated SDN-based solutions can support user mobility in dense wireless networks, making it possible to implement software in traditional and emerging wireless environments. Software-Defined Wireless Networks (SDWNs) have raised concerns about the inherent security of the SDWN architecture [125,126]. The SDWN paradigm faces security challenges akin to those present in the traditional wired SDN framework, exacerbated by the introduction of the wireless medium, which introduces additional avenues for attacks. Attackers can target the control plane, data forwarding elements, and individual wireless applications. Despite the controller's susceptibility as a single point of failure, its dynamic migration across network servers enhances resilience against potential compromises to the control plane. Furthermore, the comprehensive network visibility afforded by global monitoring empowers security administrators to monitor real-time traffic statistics and adapt security policies promptly as required.

Moreover, SDWN environments can leverage the capabilities of individual nodes to implement security at different parts of the network chain, thereby establishing a layered security model without overburdening a single network entity. Thus, if the existing centralized SDWN design is used appropriately, the framework itself can be transformed into a programmable security barrier, including functions that can be changed via programmable data plane equipment. Combining AI-related technologies with SDWNs to address SDWN security issues, integrating historical data analysis to predict malicious attacks, and accurately and effectively improving SDWN security and reliability are crucial. In SDWNs, ML algorithms play a vital role in managing numerous heterogeneous sensor nodes, optimizing each node's resource utilization, and flexibly and efficiently scheduling communication links. Currently, routing optimization, node clustering, and data aggregation in wireless sensor networks, event detection and query processing, positioning, intrusion detection, fault detection, and other problems use ML technology [127].

g. WiFi

The authors in [128] propose integrating SDN and ML techniques to improve operational efficiency and QoS in wireless local area networks (WLANs). This offers an innovative approach to wireless network management, enabling dynamic adaptation and smarter, data-driven decision-making. The second study [129] provides a comprehensive overview of advances in optimizing wireless networks through SDN and AI techniques, highlighting the potential benefits of this integration, including improved performance, efficiency, and security of WiFi networks. Finally, Ref. [130] presents a specific approach using an ML-based SDN controller for managing wireless LANs. This proposed model uses ML algorithms to optimize resource allocation and enhance WiFi network performance, demonstrating AI's potential to optimize network operations in wireless environments. Collectively, these studies emphasize the crucial role of integrating SDN and AI in the evolution of wireless networks, opening new opportunities for continuous performance and efficiency improvement [131]. WiFi challenges with ISDN include refining AI algorithms for more dynamic optimization, ensuring data security and privacy, exploring the scalability and interoperability of proposed solutions, and experimentally validating their effectiveness in wireless network environments.

h. Other Application Trends for ISDNs

The convergence of diverse advanced technologies is transforming industrial IoT and cloud computing, optimizing the efficiency and reliability of productive services, and managing critical infrastructures. Four key approaches stand out in this field.

The authors of [132] introduce a precision mechanism to allocate resources in edge computing, improving operational efficiency in smart cities. This approach allows an adaptive and dynamic response to changing demands, ensuring optimal management of urban resources. In [133], the authors address semantic segmentation in networks (Unmanned Aerial Vehicle—UAV). Techniques such as convolutional neural networks and generative adversarial networks correct biases in training data, improving the accuracy and reliability of segmentation models. Additionally, in [134], researchers apply deep neural evolution networks to detect faults in the interconnection of cloud data centers. This method combines deep learning and evolutionary algorithms, allowing accurate and timely identification of failures, as well as improving operational resilience. Finally, in [135], the authors explore the use of federated learning for productive service procurement in industrial IoT. This approach, inspired by the human brain, facilitates decentralized learning, preserves data privacy, and improves the efficiency and security of industrial processes. Together, these developments represent a significant leap towards optimization and security in resources and services management for industrial and urban environments, highlighting the transformative potential of emerging technologies in IoT and cloud computing that can be supported by ISDN.

Considering this, Table 8 shows findings that underscore key research voids within the intersection of SDN and AI, necessitating attention in forthcoming investigations. These voids delineate domains and facets that remain incompletely examined or comprehended within the scientific discourse. Addressing these lacunae promises enhancements in the methodologies and strategies deployed, as well as a deeper comprehension of AI's relevance and efficacy within SDNs. Furthermore, bridging these gaps will facilitate the creation of more refined and sophisticated models, thereby making substantial contributions to the realm of AI as applied to SDNs.

Table 8. Research Gaps in SDN and AI.

Category	Justification	Gap	Questions for Future Researchers
Thematic Gaps	Unresolved issues in specific areas of SDN	Lack of AI algorithms for network data processing and integration with SDN	How can existing AI algorithms be adapted to address the specific challenges of SDN?
		Absence of communication models between domains in SDN	What inter-domain communication approaches could be more effective in an SDN environment?
		Need for scalability schemes for SDN	How can RL schemes improve the scalability of SDN networks?
		Lack of effective security prediction methods for SDN	How can ML models enhance threat detection and mitigation in SDN?
Geographic Gaps	Limitations in the application of SDN in different contexts	Lack of SDN implementation in specific environments such as 5G, NFV, IoT, edge computing, ICN, and wireless networks	How can SDN principles be effectively and efficiently adapted to different network contexts?

Table 8. *Cont.*

Category	Justification	Gap	Questions for Future Researchers
Interdisciplinary Gaps	Need to integrate different disciplines and technologies	Requirement for AI integration with SDN	What are the best approaches to integrating AI into the management and operation of SDN networks?
		Lack of collaboration between disciplines such as computer science, networking, and cybersecurity in the context of SDN	How can researchers from different disciplines collaborate to address the interdisciplinary challenges of SDN?
Time Gaps	Future challenges that have not yet been addressed	Need for high-quality datasets for training	How can researchers improve the availability and quality of network datasets for research?
		Lack of mature models for inter-domain communication	What approaches can be developed to improve inter-domain communication in SDN?
		Lack of effective security prediction methods for SDN	What are the most promising approaches for predicting and mitigating security threats in SDN?

Source: Self-elaboration based on the results obtained in the literature review.

Figure 2 shows a detailed analysis of annual publication trends, indicating a significant increase in research activity since 2018, with notable peaks in 2019 and 2021. This upward trend reflects the growing interest and rapid advances in integrating AI with SDN technologies. Key contributions in 2019, such as a highly cited review article that represents the synergy between machine learning algorithms and SDN concepts, exemplify the foundational work driving this field forward. Similarly, the 2021 perspective on smart city applications and vehicular intelligence systems underscores the innovative and practical applications of AI-enhanced SDN.

By comparison, the research in [12] focuses on load balancing in SDN using AI, analyzing SDN architecture, and categorizing AI-based methods for load balancing. On the other hand, this research provides a broad focus on practical applications such as smart cities and vehicular systems, while [12] offers a detailed assessment of load balancing mechanisms, highlighting challenges and future trends, with a specific focus on network efficiency and resource usage. Both studies underline the importance of AI improving SDN performance, although ours provides a broader view of practical and emerging applications.

Otherwise, this research emphasizes the integration of AI in network management and its innovative applications in various sectors. In contrast, the research on the era of generative AI in 6G wireless intelligence addresses the challenges and developments in next-generation wireless networks, highlighting the role of generative AI in improving 6G network intelligence [59]. Also, it is important to emphasize that this research focuses on the synergy between AI and SDN, including applications in smart cities and vehicular systems. The research in 6G explores new fronts of wireless intelligence, covering the evolution of infrastructure and the development of advanced algorithms for 6G networks. Finally, the research in [33] focuses on the problem of controller placement during SDN deployment in telecommunication internet service provider networks, analyzing strategies to optimize controller placement to improve network performance and efficiency. Contrasting with the obtained results of this research, the integration of AI to improve network management and practical applications is highlighted.

Thus, it becomes evident that the integration of AI with SDN not only enhances network management capabilities but also paves the way for innovative applications across various sectors. However, the exploration of AI-driven SDN is still in its early stages, particularly in the context of emerging technologies such as 6G wireless intelligence. As this field continues to evolve, challenges of scalability, security, and real-time optimization remain paramount. Future research should aim to bridge these gaps by developing robust AI models tailored to the dynamic and complex nature of SDN environments, unlocking the full potential of intelligent network management systems.

Finally, and from the research results, several promising directions for future investigations in the field of AI-integrated SDN can be outlined. First, the scalability and efficiency of AI algorithms in SDN environments need to be further explored, especially in large-scale contexts such as telecommunication networks and data centers. Secondly, future research could focus on developing AI models that optimize routing and load balancing in real-time, dynamically adapting to changing network traffic conditions. Furthermore, given the growing interest in 6G wireless intelligence, the integration of generative AI to improve wireless network security and management represents another crucial area of research. It is also essential to investigate the interoperability and integration of SDN with other emerging technologies, such as edge computing and virtualized function networks, in order to create more robust and efficient systems. Finally, developing high-quality data sets and creating advanced predictive models for threat detection and cyberattack mitigation in SDN networks are critical areas that require attention to ensure the security and resilience of future network infrastructures.

5. Conclusions

This article conducts a comprehensive analysis and investigation of the application of AI technology to SDN. First, the backgrounds of AI technology and SDNs are analyzed, detailing and hierarchically describing the current state of research in both technologies. Related research on the application of AI to the data plane, control plane, and application plane of SDN is then explored. From the perspective of background and standardization of applications, current AI applications in SDN, intelligent routing optimization methods, intelligent network security methods, and AI-based methods are analyzed in detail. Related research on traffic engineering is reviewed, comparing the advantages and disadvantages of existing methods in the aforementioned research fields and providing the AI-based SDN standardization definition from the currently most authoritative international standardization organization.

The analysis of the correlation between key terms reveals the interconnection of concepts such as AI, SDN, network security, and resource management, suggesting increasing integration of these technologies to address complex issues in communications. In terms of the relevance and development of key terms, some terms, such as denial of service attacks, support vector machines, and distributed denial of service, are highly developed and relevant today, indicating significant attention in these areas. Conversely, emerging terms like AI-supported SDN and network security show growing relevance, suggesting promising and evolving research areas within the field.

Regarding traffic classification, there is a trend towards the use of AI methods due to their ability to adapt to traffic changes more effectively than traditional methods. However, the challenge remains to develop AI algorithms that can handle the increasing temporal and spatial complexity of network traffic. Route optimization is another critical aspect of SDN network design, aiming to find optimal routing solutions in real time. While heuristic methods have been widely used in the past, the potential of AI algorithms to provide more stable and efficient solutions is recognized, especially in dynamic and complex network environments. Finally, network security emerges as a central concern, where the application of AI techniques for threat detection and prevention can enhance network resilience and robustness. However, challenges related to timeliness and data reuse need to be addressed, along with the continuous evolution of attack strategies.

The evolution of artificial intelligence (AI), from its emergence in the 1950s to the present, reveals three distinct waves. Initially, AI focused on solving specific problems with heuristic rules, showing limitations in scalability and adaptability. The second wave, starting in the 1980s, was characterized by supervised, unsupervised, and semi-supervised learning, allowing systems to extract rules and patterns from observational data. These technologies, such as natural language processing and computer vision, became AI pillars. The third wave, marked by deep learning, has enabled significant advances in AI, especially in voice and image recognition, solving more complex problems.

In the context of software-defined networks (SDNs), AI integration has opened new possibilities for improving efficiency and security. In the data plane, research focuses on designing switches and forwarding rules for faster and more scalable data flow processing. In the control plane, AI application centers on optimizing routing algorithms and enhancing security through historical data-based attack detection and prevention. Lastly, in the application plane, AI is used to predict and manage traffic more efficiently, improving SDN network performance and flexibility. Concepts like the P4 programming language and combining AI and telemetry are also being explored to enhance SDN network management and performance. Additionally, key methods and technologies have been identified, such as intelligent route optimization, reinforcement learning-based routing strategies, and AI-based intrusion detection. The importance of AI-based traffic engineering for improving SDN network performance is also highlighted. However, challenges such as adaptation to specific application requirements, network security, and accurate traffic prediction need to be addressed.

Possible challenges identified include data quality, inter-domain communication, scalability, and security prediction. There is a need to adapt existing AI algorithms to specifically address SDN issues and to develop solutions tailored to different network contexts, such as 5G, network function virtualization, IoT, edge computing, information center networks, and wireless networks. Identified research gaps highlight the need for continued investigation and development of new solutions to enhance SDN and AI integration and address emerging challenges in the field of communication networks.

Regarding potential research limitations, despite the extensive coverage provided in the systematic literature review on the intersection of SDN and AI, possible publication bias, variability in the methodological quality of included studies, limited generalization of results, and lack of depth in certain research areas must be considered, potentially influencing the overall understanding of the current state of these technologies. As potential future research directions, fostering greater interdisciplinary collaboration among researchers from different fields, establishing standards and best practices, evaluating the impact in real network environments, developing specific tools and frameworks, and addressing ethical and security considerations are essential. This will enable more effective and ethical implementation of these technologies in the communications industry. An agenda that prioritizes the use of AI techniques, the development of application programs, and the continuous exploration of SDN is proposed to maintain the relevance and effectiveness of these technologies in the future.

Finally, this study presents some advantages of AI-based SDN in high-quality data, as well as the challenges they face in domain communication, scalability, and network security prediction. Based on this, AI-based SDN and emerging fields such as 5G, network function virtualization, IoT, edge computing, information center networks, and the development trend of integration in the wireless networks field are discussed. It is hoped that through the discussion and exploration in this article, a new path for research in the development of AI-based SDN will be opened, leading to the realization of smarter networks. However, it is important to note that challenges persist that need to be addressed to fully leverage the potential of this emerging technology. This includes developing more advanced AI algorithms, improving interoperability between different network components, and continuously adapting to changing network demands and threats.

Author Contributions: Conceptualization, B.J.O.C., A.O.M.B., J.D.G.B. and Á.S.; methodology, V.G.P.; software, V.G.P.; validation, B.J.O.C., A.O.M.B., J.D.G.B., Á.S. and R.A.J.; formal analysis, B.J.O.C.; investigation, B.J.O.C. and V.G.P.; resources, R.A.J.; data curation, Á.S.; writing—original draft preparation, B.J.O.C.; writing—review and editing, V.G.P.; visualization, V.G.P.; supervision, Á.S. and A.O.M.B., project administration, R.A.J., J.D.G.B. and Á.S.; funding acquisition, R.A.J. All authors have read and agreed to the published version of the manuscript.

Funding: The development of this research was supported by the ULPGC—University of Las Palmas de Gran Canaria in the discount voucher received for the APC payment of this article and also the Higher Education Institution Unidades Tecnológica de Santander (UTS) provided support in payment of 50% of the APC of this item.

Data Availability Statement: The data may be provided free of charge to interested readers by requesting the correspondence author's email.

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

References

1. Casas-Velasco, D.M.; Rendon, O.M.C.; Da Fonseca, N.L.S. Intelligent Routing Based on Reinforcement Learning for Software-Defined Networking. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 870–881. [CrossRef]
2. Lavanya, A.; Priya, N.S. Enriched Model of Case Based Reasoning and Neutrosophic Intelligent System for DDoS Attack Defence in Software Defined Network Based Cloud. *Int. J. Recent Innov. Trends Comput. Commun.* **2023**, *11*, 141–148. [CrossRef]
3. Amin, R.; Reisslein, M.; Shah, N. Hybrid SDN Networks: A Survey of Existing Approaches. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3259–3306. [CrossRef]
4. Dinh, K.T.; Kukliński, S.; Osiński, T.; Wytrębowicz, J. Heuristic Traffic Engineering for SDN. *J. Inf. Telecommun.* **2020**, *4*, 251–266. [CrossRef]
5. Gazi, F.; Ahmed, N.; Misra, S.; Tiwari, M.K. ProStream: Programmable Underwater IoT Network for Multimedia Streaming. *IEEE Internet Things J.* **2022**, *9*, 17417–17424. [CrossRef]
6. Cui, L.; Yu, F.R.; Yan, Q. When Big Data Meets Software-Defined Networking: SDN for Big Data and Big Data for SDN. *IEEE Netw.* **2016**, *30*, 58–65. [CrossRef]
7. Jimenez, M.B.; Fernandez, D.; Rivadeneira, J.E.; Bellido, L.; Cardenas, A. A Survey of the Main Security Issues and Solutions for the SDN Architecture. *IEEE Access* **2021**, *9*, 122016–122038.
8. Gilani, S.S.A.; Qayyum, A.; Rais, R.N.B.; Bano, M. SDNMesh: An SDN Based Routing Architecture for Wireless Mesh Networks. *IEEE Access* **2020**, *8*, 136769–136781. [CrossRef]
9. Haseeb, K.; Ahmad, I.; Awan, I.I.; Lloret, J.; Bosch, I. A Machine Learning Sdn-Enabled Big Data Model for Iomt Systems. *Electronics* **2021**, *10*, 2228. [CrossRef]
10. Khan, M.; Iqbal, J.; Talha, M.; Arshad, M.; Diyan, M.; Han, K. Big Data Processing Using Internet of Software Defined Things in Smart Cities. *Int. J. Parallel Program.* **2020**, *48*, 178–191. [CrossRef]
11. Babbar, H.; Rani, S.; Alqahtani, S.A. Intelligent Edge Load Migration in SDN-IIoT for Smart Healthcare. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8058–8064. [CrossRef]
12. Alhilali, A.H.; Montazerolghaem, A. Artificial Intelligence Based Load Balancing in SDN: A Comprehensive Survey. *Internet Things* **2023**, *22*, 100814. [CrossRef]
13. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Int. J. Surg.* **2021**, *88*, 105906. [CrossRef]
14. Exterior, C.; Guillermina Moncada-Hernández, S. Cómo Realizar Una Búsqueda de Información Eficiente. *Investig. Educ. Médica* **2014**, *3*, 106–115.
15. Zhao, Y.; Li, Y.; Zhang, X.; Geng, G.; Zhang, W.; Sun, Y. A Survey of Networking Applications Applying the Software Defined Networking Concept Based on Machine Learning. *IEEE Access* **2019**, *7*, 95397–95417. [CrossRef]
16. Latah, M.; Toker, L. Artificial Intelligence Enabled Software-defined Networking: A Comprehensive Overview. *IET Netw.* **2019**, *8*, 79–99. [CrossRef]
17. Rani, P.; Hussain, N.; Khan, R.A.H.; Sharma, Y.; Shukla, P.K. Vehicular Intelligence System: Time-Based Vehicle Next Location Prediction in Software-Defined Internet of Vehicles (SDN-IOV) for the Smart Cities. In *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*; Springer International Publishing: Cham, Switzerland, 2021; pp. 35–54.
18. Anyanwu, G.O.; Nwakanma, C.I.; Lee, J.-M.; Kim, D.-S. RBF-SVM Kernel-Based Model for Detecting DDoS Attacks in SDN Integrated Vehicular Network. *Ad Hoc Netw.* **2023**, *140*, 103026. [CrossRef]
19. Hassen, H.; Meherzi, S.; Jemaa, Z. Ben Improved Exploration Strategy for Q-Learning Based Multipath Routing in SDN Networks. *J. Netw. Syst. Manag.* **2024**, *32*, 25. [CrossRef]
20. Wu, H.; Chen, J.; Zhou, C.; Shi, W.; Cheng, N.; Xu, W.; Zhuang, W.; Shen, X.S. Resource Management in Space-Air-Ground Integrated Vehicular Networks: SDN Control and AI Algorithm Design. *IEEE Wirel. Commun.* **2020**, *27*, 52–60. [CrossRef]
21. Belgaum, M.R.; Musa, S.; Alam, M.M.; Su'ud, M.M. A Systematic Review of Load Balancing Techniques in Software-Defined Networking. *IEEE Access* **2020**, *8*, 98612–98636. [CrossRef]
22. Belgaum, M.R.; Alansari, Z.; Musa, S.; Mansoor Alam, M.; Mazliham, M.S. Role of Artificial Intelligence in Cloud Computing, IoT and SDN: Reliability and Scalability Issues. *Int. J. Electr. Comput. Eng. (IJECE)* **2021**, *11*, 4458. [CrossRef]
23. Riyaz Belgaum, M.; Ali, F.; Alansari, Z.; Musa, S.; Mansoor Alam, M.; Mazliham, M.S. Artificial Intelligence Based Reliable Load Balancing Framework in Software-Defined Networks. *Comput. Mater. Contin.* **2022**, *70*, 251–266. [CrossRef]

24. Belgaum, M.R.; Alansari, Z.; Musa, S.; Alam, M.M.; Mazliham, M.S. Impact of Artificial Intelligence-Enabled Software-Defined Networks in Infrastructure and Operations: Trends and Challenges. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 231983024. [CrossRef]
25. Shinde, A.R.; Bendale, S.P. Implications and Application of Artificial Intelligence and Machine Learning Concepts on Software Defined Network and Its Future Prospects. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 1142–1152.
26. Liu, C.-H.; Yeh, Y.-T. The Study of SDN for Campus Security. In Proceedings of the 2015 IEEE International Conference on Consumer Electronics, Taipei, Taiwan, 6–8 June 2015; IEEE: New York, NY, USA, 2015; pp. 428–429.
27. Lu, X.; Chen, J.; Lu, L.; Huang, X.; Lu, X. SDN Routing Optimization Based on Improved Reinforcement Learning. In Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, Guangzhou, China, 4–6 December 2020; ACM: New York, NY, USA, 2020; pp. 153–158.
28. Xiangyun, Z.; Lijun, W.; Zhiyuan, L.; Yulin, J. Deep Reinforcement Learning with Graph Convolutional Networks for Load Balancing in SDN-Based Data Center Networks. In Proceedings of the 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 17–19 December 2021; IEEE: New York, NY, USA, 2021; pp. 344–352.
29. Abbas, S.O.; Alenazi, M.J.F. SSHS: SDN Seamless Handover System among LAN Access Points. *Concurr. Comput.* **2023**, *35*, e7821. [CrossRef]
30. Krishnan, P.; Jain, K.; Aldweesh, A.; Prabu, P.; Buyya, R. OpenStackDP: A Scalable Network Security Framework for SDN-Based OpenStack Cloud Infrastructure. *J. Cloud Comput.* **2023**, *12*, 26. [CrossRef]
31. Awan, K.A.; Din, I.U.; Almogren, A.; Rodrigues, J.J.P.C. Artificial Intelligence and Quantum Synergies in Trust-Enhanced Consumer Applications for Software Defined Networks. *IEEE Trans. Consum. Electron.* **2024**, *70*, 791–799. [CrossRef]
32. Liu, B.; Yang, B.; Sun, R.; Liang, Z.; Sun, Z.; Li, Z. Intelligent SDN Routing: A Threshold-Based and LSTM-Enhanced Deep Q-Network Routing Algorithm. In Proceedings of the 2023 International Conference on Electronics, Computers and Communication Technology, Nanning, China, 21–23 July 2023; ACM: New York, NY, USA, 2023; pp. 188–195.
33. Sapkota, B.; Dawadi, B.R.; Joshi, S.R. Controller Placement Problem during SDN Deployment in the ISP/Telco Networks: A Survey. *Eng. Rep.* **2024**, *6*, e12801. [CrossRef]
34. Yankam, Y.F.; Tchendji, V.K.; Myoupo, J.F. WoS-CoMS: Work Stealing-Based Congestion Management Scheme for SDN Programmable Networks. *J. Netw. Syst. Manag.* **2024**, *32*, 23. [CrossRef]
35. Zhang, W.; Wu, Z.; Wei, Q.; Yuan, H. A Systematic Treat Model for Software-Defined Networking. *KSII Trans. Internet Inf. Syst.* **2021**, *15*, 580–599. [CrossRef]
36. Kaliyamurthy, N.M.; Taterh, S.; Shanmugasundaram, S.; Saxena, A.; Cheikhrouhou, O.; Ben Elhadj, H. Software-Defined Networking: An Evolving Network Architecture—Programmability and Security Perspective. *Secur. Commun. Netw.* **2021**, *2021*, 9971705. [CrossRef]
37. Glenn Brown 7 Advantages of Software Defined Networking. Available online: https://www.cablelabs.com/blog/nfv-and-sdn-paving-the-way-to-a-software-based-networking-future (accessed on 17 June 2024).
38. Fu, Q.; Sun, E.; Sun, E.; Meng, K.; Li, M.; Zhang, Y. Deep Q-Learning for Routing Schemes in SDN-Based Data Center Networks. *IEEE Access* **2020**, *8*, 103491–103499. [CrossRef]
39. Haxhibeqiri, J.; Isolani, P.H.; Marquez-Barja, J.M.; Moerman, I.; Hoebeke, J. In-Band Network Monitoring Technique to Support SDN-Based Wireless Networks. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 627–641. [CrossRef]
40. Son, J.; Buyya, R. A Taxonomy of Software-Defined Networking (SDN)-Enabled Cloud Computing. *ACM Comput. Surv.* **2018**, *51*, 59. [CrossRef]
41. Dong, S.; Abbas, K.; Jain, R. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access* **2019**, *7*, 80813–80828. [CrossRef]
42. Capdevila-Werning, R. Open Networking Foundation. SDN Architecture. 2018. Available online: https://openupeu.com/personnel/remei-capdevila-werning/ (accessed on 17 June 2024).
43. Batz, P.; Will, T.; Thiel, S.; Ziesche, T.M.; Joachim, C. From Identification to Forecasting: The Potential of Image Recognition and Artificial Intelligence for Aphid Pest Monitoring. *Front. Plant Sci.* **2023**, *14*, 1150748. [CrossRef]
44. Ibn-Khedher, H.; Laroui, M.; Moungla, H.; Afifi, H.; Abd-Elrahman, E. Next-Generation Edge Computing Assisted Autonomous Driving Based Artificial Intelligence Algorithms. *IEEE Access* **2022**, *10*, 53987–54001. [CrossRef]
45. Marik, V.; Zdrahal, Z. Pattern Recognition and Artificial Intelligence. *Signal Process.* **1980**, *2*, 81. [CrossRef]
46. Kakani, V.; Nguyen, V.H.; Kumar, B.P.; Kim, H.; Pasupuleti, V.R. A Critical Review on Computer Vision and Artificial Intelligence in Food Industry. *J. Agric. Food Res.* **2020**, *2*, 100033. [CrossRef]
47. Olveres, J.; González, G.; Torres, F.; Moreno-Tagle, J.C.; Carbajal-Degante, E.; Valencia-Rodríguez, A.; Méndez-Sánchez, N.; Escalante-Ramírez, B. What Is New in Computer Vision and Artificial Intelligence in Medical Image Analysis Applications. *Quant. Imaging Med. Surg.* **2021**, *11*, 3830. [CrossRef]
48. Jia, Z.; Lin, Y.; Wang, J.; Wang, X.; Xie, P.; Zhang, Y. SalientSleepNet: Multimodal Salient Wave Detection Network for Sleep Staging. In Proceedings of the IJCAI International Joint Conference on Artificial Intelligence, Montreal, QC, Canada, 19–27 August 2021.
49. Kim, H.R.; Sung, M.; Park, J.A.; Jeong, K.; Kim, H.H.; Lee, S.; Park, Y.R. Analyzing Adverse Drug Reaction Using Statistical and Machine Learning Methods: A Systematic Review. *Medicine* **2022**, *101*, e29387. [CrossRef]
50. Rani, V.; Nabi, S.T.; Kumar, M.; Mittal, A.; Kumar, K. Self-Supervised Learning: A Succinct Review. *Arch. Comput. Methods Eng.* **2023**, *30*, 2761–2775. [CrossRef] [PubMed]

51. Naeem, S.; Ali, A.; Anam, S.; Ahmed, M.M. An Unsupervised Machine Learning Algorithms: Comprehensive Review. *Int. J. Comput. Digit. Syst.* **2023**, *13*, 911–921. [CrossRef]
52. C A Padmanabha Reddy, Y.; Viswanath, P.; Eswara Reddy, B. Semi-Supervised Learning: A Brief Review. *Int. J. Eng. Technol.* **2018**, *7*, 81. [CrossRef]
53. Low, Y.; Gonzalez, J.; Kyrola, A.; Bickson, D.; Guestrin, C.; Hellerstein, J.M. Distributed GraphLab: A Framework for Machine Learning and Data Mining in the Cloud. *Proc. VLDB Endow.* **2012**, *5*, 716. [CrossRef]
54. Shrestha, A.; Mahmood, A. Review of Deep Learning Algorithms and Architectures. *IEEE Access* **2019**, *7*, 53040–53065. [CrossRef]
55. Deng, L. Deep Learning: From Speech Recognition to Language and Multimodal Processing. *APSIPA Trans. Signal Inf. Process.* **2016**, *5*, e1.
56. Shafiq, M.; Gu, Z. Deep Residual Learning for Image Recognition: A Survey. *Appl. Sci.* **2022**, *12*, 8972. [CrossRef]
57. Sarker, I.H. LLM potentiality and awareness: A position paper from the perspective of trustworthy and responsible AI modeling. *Discov. Artif. Intell.* **2024**, *4*, 40. [CrossRef]
58. Sarker, I.H. Data Science and Analytics: An Overview from Data-Driven Smart Computing, Decision-Making and Applications Perspective. *SN Comput. Sci.* **2021**, *2*, 377. [CrossRef]
59. Celik, A.; Eltawil, A.M. At the Dawn of Generative AI Era: A Tutorial-cum-Survey on New Frontiers in 6G Wireless Intelligence. *IEEE Open J. Commun. Soc.* **2024**, *5*, 2433–2489. [CrossRef]
60. Arkhangelskaya, E.O.; Nikolenko, S.I. Deep Learning for Natural Language Processing: A Survey. *J. Math. Sci.* **2023**, *273*, 533–582. [CrossRef]
61. Etengu, R.; Tan, S.C.; Kwang, L.C.; Abbou, F.M.; Chuah, T.C. AI-Assisted Framework for Green-Routing and Load Balancing in Hybrid Software-Defined Networking: Proposal, Challenges and Future Perspective. *IEEE Access* **2020**, *8*, 166384–166441. [CrossRef]
62. Kawashima, R.; Nakayama, H.; Hayashi, T.; Matsuo, H. Evaluation of Forwarding Efficiency in NFV-Nodes toward Predictable Service Chain Performance. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 920–933. [CrossRef]
63. Khan, N.; Salleh, R.B.; Koubaa, A.; Khan, Z.; Khan, M.K.; Ali, I. Data Plane Failure and Its Recovery Techniques in SDN: A Systematic Literature Review. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 176–201. [CrossRef]
64. Zheng, S.; Yang, S. Application of SDN Network Traffic Prediction Based on Speech Recognition in Educational Information Optimization Platform. *Comput. Intell. Neurosci.* **2022**, *2022*, 5716698. [CrossRef]
65. Pandey, S.; Srivastava, A.K.; Amidan, B.G. A Real Time Event Detection, Classification and Localization Using Synchrophasor Data. *IEEE Trans. Power Syst.* **2020**, *35*, 4421–4431. [CrossRef]
66. Tang, F.; Fadlullah, Z.M.; Mao, B.; Kato, N. An Intelligent Traffic Load Prediction-Based Adaptive Channel Assignment Algorithm in SDN-IoT: A Deep Learning Approach. *IEEE Internet Things J.* **2018**, *5*, 5141–5154. [CrossRef]
67. Khairi, M.H.H.; Ariffin, S.H.S.; Latiff, N.M.A.A.; Yusof, K.M.; Hassan, M.K.; Al-Dhief, F.T.; Hamdan, M.; Khan, S.; Hamzah, M. Detection and Classification of Conflict Flows in SDN Using Machine Learning Algorithms. *IEEE Access* **2021**, *9*, 76024–76037. [CrossRef]
68. Hussain, M.; Shah, N.; Amin, R.; Alshamrani, S.S.; Alotaibi, A.; Raza, S.M. Software-Defined Networking: Categories, Analysis, and Future Directions. *Sensors* **2022**, *22*, 5551. [CrossRef]
69. Sherjah, P.Y.; Sajikumar, N.; Nowshaja, P.T. Quality Monitoring of Inland Water Bodies Using Google Earth Engine. *J. Hydroinform.* **2023**, *25*, 432–450. [CrossRef]
70. Bu, S.J.; Kim, H.J. Optimized URL Feature Selection Based on Genetic-Algorithm-Embedded Deep Learning for Phishing Website Detection. *Electronics* **2022**, *11*, 1090. [CrossRef]
71. Fatani, A.; Elaziz, M.A.; Dahou, A.; Al-Qaness, M.A.A.; Lu, S. IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization. *IEEE Access* **2021**, *9*, 123448–123464. [CrossRef]
72. Hou, Y.; Teo, S.G.; Chen, Z.; Wu, M.; Kwoh, C.K.; Truong-Huu, T. Handling Labeled Data Insufficiency: Semi-Supervised Learning with Self-Training Mixup Decision Tree for Classification of Network Attacking Traffic. *IEEE Trans. Dependable Secur. Comput.* **2022**, 1–14. [CrossRef]
73. Soysal, M.; Schmidt, E.G. Machine Learning Algorithms for Accurate Flow-Based Network Traffic Classification: Evaluation and Comparison. *Perform. Eval.* **2010**, *67*, 451–467. [CrossRef]
74. Musumeci, F.; Fidanci, A.C.; Paolucci, F.; Cugini, F.; Tornatore, M. Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks. *J. Netw. Syst. Manag.* **2022**, *30*, 21. [CrossRef]
75. Mozo, A.; Karamchandani, A.; de la Cal, L.; Gómez-Canaval, S.; Pastor, A.; Gifre, L. A Machine-Learning-Based Cyberattack Detector for a Cloud-Based SDN Controller. *Appl. Sci.* **2023**, *13*, 4914. [CrossRef]
76. Zanna, P.; Radcliffe, P.; Kumar, D. Preventing Attacks on Wireless Networks Using SDN Controlled OODA Loops and Cyber Kill Chains. *Sensors* **2022**, *22*, 9481. [CrossRef]
77. López-Millán, G.; Marín-López, R.; Pereñíguez-García, F.; Canovas, O.; Parra Espín, J.A. Analysis and Practical Validation of a Standard SDN-Based Framework for IPsec Management. *Comput. Stand. Interfaces* **2023**, *83*, 103665. [CrossRef]
78. Carvajal, J.M.; Gilabert, F.T.; Canadas, J. Corporate Network Transformation with SD-WAN. A Practical Approach. In Proceedings of the 2021 8th International Conference on Software Defined Systems, SDS 2021, Gandia, Spain, 6–9 December 2021.
79. Al Mhdawi, A.K.; Al-Raweshidy, H.S. IPRDR: Intelligent Power Reduction Decision Routing Protocol for Big Traffic Flood in Hybrid-SDN Architecture. *IEEE Access* **2018**, *6*, 10944–10955. [CrossRef]

80. Chen, Y.; Lv, K.; Hu, C. A Dynamic Hidden Forwarding Path Planning Method Based on Improved Q-Learning in SDN Environments. *Secur. Commun. Netw.* **2018**, *2018*, 2058429. [CrossRef]
81. Sharathkumar, S.; Sreenath, N. HSPC-SDN: Heuristic Driven Self-Configuring Proactive Controller for QoS-Centric Software Defined Network. *Int. J. Comput. Digit. Syst.* **2023**, *13*, 203–222. [CrossRef]
82. Finogeev, A.; Deev, M.; Parygin, D.; Finogeev, A. Intelligent SDN Architecture with Fuzzy Neural Network and Blockchain for Monitoring Critical Events. *Appl. Artif. Intell.* **2022**, *36*, 2145634. [CrossRef]
83. Kumar, R.; Venkanna, U.; Tiwari, V. Optimized Traffic Engineering in Software Defined Wireless Network Based IoT (SDWN-IoT): State-of-the-Art, Research Opportunities and Challenges. *Comput. Sci. Rev.* **2023**, *49*, 100572. [CrossRef]
84. Jurado-Lasso, F.F.; Clarke, K.; Cadavid, A.N.; Nirmalathas, A. Energy-Aware Routing for Software-Defined Multihop Wireless Sensor Networks. *IEEE Sens. J.* **2021**, *21*, 10174–10182. [CrossRef]
85. Wang, J.; Feng, Q.; Ma, J.; Feng, Y. FL-SDUAN: A Fuzzy Logic-Based Routing Scheme for Software-Defined Underwater Acoustic Networks. *Appl. Sci.* **2023**, *13*, 944. [CrossRef]
86. Musa, N.S.; Mirza, N.M.; Rafique, S.H.; Abdallah, A.M.; Murugan, T. Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks—Current Research Solutions. *IEEE Access* **2024**, *12*, 17982–18011. [CrossRef]
87. Hou, J.; Tao, T.; Lu, H.; Nayak, A. Intelligent Caching with Graph Neural Network-Based Deep Reinforcement Learning on SDN-Based ICN. *Future Internet* **2023**, *15*, 251. [CrossRef]
88. Farris, I.; Taleb, T.; Khettab, Y.; Song, J. A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 812–837. [CrossRef]
89. Alamri, H.A.; Thayananthan, V.; Yazdani, J. Machine Learning for Securing SDN Based 5G Network. *Int. J. Comput. Appl.* **2021**, *174*, 9–16. [CrossRef]
90. Kumar, G.; Alqahtani, H. Machine Learning Techniques for Intrusion Detection Systems in SDN-Recent Advances, Challenges and Future Directions. *CMES—Comput. Model. Eng. Sci.* **2023**, *134*, 89–119. [CrossRef]
91. Santos Da Silva, A.; Wickboldt, J.A.; Granville, L.Z.; Schaeffer-Filho, A. ATLANTIC: A Framework for Anomaly Traffic Detection, Classification, and Mitigation in SDN. In Proceedings of the NOMS 2016—2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 25–29 April 2016.
92. Karnani, S.; Shakya, H.K. Mitigation Strategies for Distributed Denial of Service (DDoS) in SDN: A Survey and Taxonomy. *Inf. Secur. J.* **2023**, *32*, 444–468. [CrossRef]
93. Niyaz, Q.; Sun, W.; Javaid, A.Y. A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN). *ICST Trans. Secur. Saf.* **2017**, *12*, e2. [CrossRef]
94. Chen, Z.; Jiang, F.; Cheng, Y.; Gu, X.; Liu, W.; Peng, J. XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-Based Cloud. In Proceedings of the 2018 IEEE International Conference on Big Data and Smart Computing, BigComp, Shanghai, China, 15–17 January 2018.
95. Al-Saadi, M.; Khan, A.; Kelefouras, V.; Walker, D.J.; Al-Saadi, B. SDN-Based Routing Framework for Elephant and Mice Flows Using Unsupervised Machine Learning. *Network* **2023**, *3*, 218–238. [CrossRef]
96. Karakus, M.; Durresi, A. Quality of Service (QoS) in Software Defined Networking (SDN): A Survey. *J. Netw. Comput. Appl.* **2017**, *80*, 200–218. [CrossRef]
97. Binsahaq, A.; Sheltami, T.R.; Salah, K. A Survey on Autonomic Provisioning and Management of QoS in SDN Networks. *IEEE Access* **2019**, *7*, 73384–73435. [CrossRef]
98. Liu, W.X.; Cai, J.; Wang, Y.; Chen, Q.C.; Zeng, J.Q. Fine-Grained Flow Classification Using Deep Learning for Software Defined Data Center Networks. *J. Netw. Comput. Appl.* **2020**, *168*, 102766. [CrossRef]
99. Galluccio, L.; Grasso, C.; Grasso, M.; Raftopoulos, R.; Schembra, G. Measuring QoS and QoE for a Softwarized Video Surveillance System in a 5G Network. In Proceedings of the 2019 IEEE International Symposium on Measurements and Networking (M&N), Catania, Italy, 8–10 July 2019.
100. Wang, L. A Traffic Scheduling Method Based on SDN. *Math. Probl. Eng.* **2022**, *2022*, 1819202. [CrossRef]
101. Jing, L.; Chen, X.; Wang, J. Design and Implementation of Programmable Data Plane Supporting Multiple Data Types. *Electronics* **2021**, *10*, 2639. [CrossRef]
102. Azzouni, A.; Boutaba, R.; Pujolle, G. NeuRoute: Predictive Dynamic Routing for Software-Defined Networks. In Proceedings of the 2017 13th International Conference on Network and Service Management, CNSM 2017, Tokyo, Japan, 26–30 November 2017.
103. Soud, N.S.; Al-Jamali, N.A.S.; Al-Raweshidy, H.S. Moderately Multispike Return Neural Network for SDN Accurate Traffic Awareness in Effective 5G Network Slicing. *IEEE Access* **2022**, *10*, 73378–73387. [CrossRef]
104. Kafetzis, D.; Vassilaras, S.; Vardoulias, G.; Koutsopoulos, I. Software-Defined Networking Meets Software-Defined Radio in Mobile Ad Hoc Networks: State of the Art and Future Directions. *IEEE Access* **2022**, *10*, 9989–10014. [CrossRef]
105. Karakus, M.; Durresi, A. A Survey: Control Plane Scalability Issues and Approaches in Software-Defined Networking (SDN). *Comput. Netw.* **2017**, *112*, 279–293. [CrossRef]
106. Zobary, F.; ChunLin, L. A Mathematical Model for SDN Control Plane Scalability Evaluation Based on Controller Utilization. *Control. Eng. Appl. Inform.* **2023**, *25*, 14–21. [CrossRef]
107. Linhares, T.; Patel, A.; Barros, A.L.; Fernandez, M. SDNTruth: Innovative DDoS Detection Scheme for Software-Defined Networks (SDN). *J. Netw. Syst. Manag.* **2023**, *31*, 55. [CrossRef]

108. Wang, P.; Wang, Z.; Ye, F.; Chen, X. ByteSGAN: A Semi-Supervised Generative Adversarial Network for Encrypted Traffic Classification in SDN Edge Gateway. *Comput. Netw.* **2021**, *200*, 108535. [CrossRef]
109. Sermpezis, P.; Dimitropoulos, X. Inter-Domain SDN: Analysing the Effects of Routing Centralization on BGP Convergence Time. *ACM SIGMETRICS Perform. Eval. Rev.* **2016**, *44*, 30–32. [CrossRef]
110. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K.; Chowdhry, B.S. Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions. *Wirel. Pers. Commun.* **2023**, *130*, 2753–2800. [CrossRef]
111. 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]
112. Kelian, V.H.; Warip, M.N.M.; Ahmad, R.B.; Ehkan, P.; Zakaria, F.F.; Ilyas, M.Z. Toward Adaptive and Scalable Topology in Distributed SDN Controller. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2023**, *30*, 115–131. [CrossRef]
113. Sun, S.; Rong, B.; Hu, R.Q.; Qian, Y. Spatial Domain Management and Massive MIMO Coordination in 5G SDN. *IEEE Access* **2015**, *3*, 2238–2251. [CrossRef]
114. Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Pérez-Díaz, J.A. SDN/NFV-Based Framework for Autonomous Defense against Slow-Rate DDoS Attacks by Using Reinforcement Learning. *Future Gener. Comput. Syst.* **2023**, *149*, 637–649. [CrossRef]
115. Soussi, W.; Christopoulou, M.; Gur, G.; Stiller, B. MERLINS—Moving Target Defense Enhanced with Deep-RL for NFV In-Depth Security. In Proceedings of the 2023 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2023, Dresden, Germany, 7–9 November 2023.
116. Wu, B.; Zeng, J.; Shao, S.; Ni, W.; Tang, Y. New Game-Theoretic Approach to Decentralized Path Selection and Sleep Scheduling for Mobile Edge Computing. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 6125–6140. [CrossRef]
117. Jiang, J.; Lin, C.; Han, G.; Abu-Mahfouz, A.M.; Shah, S.B.H.; Martínez-García, M. How AI-Enabled SDN Technologies Improve the Security and Functionality of Industrial IoT Network: Architectures, Enabling Technologies, and Opportunities. *Digit. Commun. Netw.* **2023**, *9*, 1351–1362. [CrossRef]
118. Costa, B.H.G.; Rodrigues, A.W.d.O. Uma Proposta de Controlador SDN e Aprendizado de Máquina Para Detecção de Ataques Por Botnets Em Redes IoT: Uma Abordagem Para o Ensino de Redes de Computadores. In Proceedings of the Congresso Sobre Tecnologias Na Educação, Santarém, Brazil, 23–25 August 2023.
119. Kumhar, M.; Bhatia, J.B. Edge Computing in SDN-Enabled IoTBased Healthcare Frameworks: Challenges and Future Research Directions. *Int. J. E-Health Med. Commun.* **2022**, *11*, 1–15. [CrossRef]
120. Nascimento, E.B.; Moreno, E.D.; De Macedo, D.D.J.; De Bona, L.C.E.; Da Rosa Righi, R.; Messina, F. On Proposing a Novel SDN-Caching Mechanism for Optimizing Distribution in ICN Networks. *Adv. Electr. Comput. Eng.* **2023**, *23*, 61–70. [CrossRef]
121. Hamaali, K.W.; Zeebaree, S.R.M. Resources Allocation for Distributed Systems: A Review. *Int. J. Sci. Bus.* **2021**, *5*, 76–88.
122. Masood, F.; Khan, W.U.; Jan, S.U.; Ahmad, J. AI-Enabled Traffic Control Prioritization in Software-Defined IoT Networks for Smart Agriculture. *Sensors* **2023**, *23*, 8218. [CrossRef] [PubMed]
123. Zhang, Q.Y.; Wang, X.W.; Huang, M.; Li, K.Q.; Das, S.K. Software Defined Networking Meets Information Centric Networking: A Survey. *IEEE Access* **2018**, *6*, 39547–39563. [CrossRef]
124. Raschellà, A.; Eiza, M.H.; MacKay, M.; Shi, Q.; Banton, M. A Trust-Based Cooperative System for Efficient Wi-Fi Radio Access Networks. *IEEE Access* **2023**, *11*, 136136–136149. [CrossRef]
125. Li, J.; Ye, M.; Huang, L.; Deng, X.; Qiu, H.; Wang, Y.; Jiang, Q. An Intelligent SDWN Routing Algorithm Based on Network Situational Awareness and Deep Reinforcement Learning. *IEEE Access* **2023**, *11*, 83322–83342. [CrossRef]
126. Azka, N.; Revathi, S.; Geetha, A. A survey of applications and security issues in software defined networking. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 21–28. [CrossRef]
127. He, D.; Chan, S.; Guizani, M. Securing Software Defined Network against Rogue Controllers. *IEEE Commun. Mag.* 2016. Available online: https://www.researchgate.net/publication/312032629_SECURING_SOFTWARE_DEFINED_NETWORK_AGAINST_ROGUE_CONTROLLERS (accessed on 17 June 2024).
128. Jurado-Lasso, F.F.; Marchegiani, L.; Jurado, J.F.; Abu-Mahfouz, A.M.; Fafoutis, X. A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges. *IEEE Access* **2022**, *10*, 23560–23592. [CrossRef]
129. Coronado, E.; Thomas, A.; Riggio, R. Adaptive ML-Based Frame Length Optimisation in Enterprise SD-WLANs. *J. Netw. Syst. Manag.* **2020**, *28*, 850–881. [CrossRef]
130. Dhanasekar, S.; Meignanamoorthi, D.; Vetriselvi, V. Routing Optimization using Deep Reinforcement Learning in Wireless Software-Defined Edge Network. In Proceedings of the 1st International Conference on Emerging Research in Computational Science, ICERCS 2023, Coimbatore, India, 7–9 December 2023. [CrossRef]
131. Lopez-Raventos, A.; Wilhelmi, F.; Barrachina-Munoz, S.; Bellalta, B. Combining software defined networks and machine learning to enable self organizing wlans. In Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications, Barcelona, Spain, 21–23 October 2019. [CrossRef]
132. Sun, Z.; Yang, H.; Li, C.; Yao, Q.; Teng, Y.; Zhang, J.; Liu, S.; Li, Y.; Vasilakos, A.V. A Resource Allocation Scheme for Edge Computing Network in Smart City Based on Attention Mechanism. *ACM Trans. Sen. Netw.* **2024**. *accepted*. [CrossRef]
133. Yu, T.; Yang, H.; Nie, J.; Yao, Q.; Liu, W.; Zhang, J.; Cheriet, M. Bias-Compensation Augmentation Learning for Semantic Segmentation in UAV Networks. *IEEE Internet Things J.* **2024**, *11*, 21261–21273. [CrossRef]

134. Yang, H.; Zhao, X.; Yao, Q.; Yu, A.; Zhang, J.; Ji, Y. Accurate Fault Location using Deep Neural Evolution Network in Cloud Data Center Interconnection. *IEEE Trans. Cloud Comput.* **2022**, *10*, 1402–1412. [CrossRef]
135. Yang, H.; Yuan, J.; Li, C.; Zhao, G.; Sun, Z.; Yao, Q.; Bao, B.; Vasilakos, A.V.; Zhang, J. BrainIoT: Brain-Like Productive Services Provisioning With Federated Learning in Industrial IoT. *IEEE Internet Things J.* **2022**, *9*, 2014–2024. [CrossRef]

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